[The Complete] Management Solution
For Your Network

PRODUCT MANUAL

ManageWise® 2.6
InocuLAN AntiVirus Guide

ManageWise®
MANAGEMENT SOFTWARE

Novell®

disclaimer

U.S. GOVERNMENT RESTRICTED RIGHTS

The software and accompanying materials are provided with RESTRICTED RIGHTS. Use, duplication or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 subdivision (c)(1) and (2), as applicable. Contractor/manufacturer is Computer Associates International, Inc., One Computer Associates Plaza, Islandia, NY 11788-7000 (hereinafter "Computer Associates").

Computer Associates provides this publication "as is" without warranty of any kind, either expressed or implied, including but not limited to the implied warranties of merchantability or fitness for a particular purpose. The entire risk as to the use of this information is assumed by the user.

In no event will Computer Associates be liable for any damages, direct, indirect, incidental, special or consequential, resulting from any defect in the information, even if it has been advised of the possibility of such damages.

Further, Computer Associates reserves the right to revise this publication and to make changes to it from time to time without obligation to notify any person or organization of such revision or change.

trademarks

Novell, Inc. has attempted to supply trademark information about company names, products, and services mentioned in this manual. Novell and NetWare are registered trademarks of Novell, Inc. in the United States and other countries.

Cheyenne is a registered trademark of Computer Associates International, Inc. or one of its subsidiaries.

Other brand or product names used in this manual, but not listed here, are trademarks or registered trademarks of their respective holders.

StorageExpress is a trademark of Intel Corporation. IBM, OS/2, PC/AT, and PS/2 are registered trademarks and PC/XT is a trademark of International Business Machines Corporation. LANSpool is a registered trademark of LAN

Credits

Written by James Carter and Michael Liang

Edited by Alex Chen, John Gargiulo, Andrew Malitzis, Carl Oddo, and Steve Ovits. Revision: June, 1997

Product Support

If you have any questions about this product, please contact us at one of the following:

USA, Canada, Asia, Latin America:	Main Voice Number:	516-465-4000
3 Expressway Plaza	Technical Support:	800-CHEY-TEC
Roslyn Heights, New York 11577		Mon-Fri 8:00 am- 8:00 pm EST
USA		Mon-Fri 8:00 pm-10 pm EST (Callback only)
		Sat/Sun 10:00 am-4:00 pm EST (Callback only)
	Tech Support FAX:	516-465-5115
	BBS:	516-465-3900
	CompuServe:	GO CHEYENNE
	World-wide Web:	http://www.cheyenne.com/
	FTP Server:	ftp.cheyenne.com
	InfoFax System:	516-465-5979 (Outside of North America you must use a fax machine's telephone.)
European Headquarters:	Southern Europe Tech	+33-1-49-93-90-34
Cheyenne Software S.A.R.L.	Support:	Mon-Fri 09:00 - 17:00
Bel Air Building	Tech Support	
58 rue Pottier	(FAX Hot Line):	+33-1-39-23-18-69
78150 Le Chesnay, France	BBS:	+33-1-39-23-18-60
	Infofax:	+33-1-39-23-47-00
Germany:	Central and Eastern	+49-69-920321-80
Cheyenne Software Deutschland	Europe Tech Support:	Mon-Fri 09:00 - 17:00
Bayerwaldstr. 3	Tech Support FAX:	+49-89-627241-41
81737 Munich, Germany	BBS (28800,N,8,1):	+49-89-627241-80
	BBS ISDN 64kB (v110,	
	v120):	+49-89-627241-85
England:	Northern Europe Tech	+44 (0) 990 239606
Cheyenne Software (UK) LTD	Support:	Mon-Fri 09:00 - 17:00
Furness House	Tech Support FAX:	+44 (0) 990 785783
53 Brighton Road	BBS:	+44 (0) 990 143012
Redhill, Surrey, England RH1 6PZ		
Japan:	Voice:	+81-3-3222-3760
Cheyenne Software K.K.	FAX:	+81-3-3222-3762
Sumitomo Fudosan Sanbancho Bldg.		
3F, 6-26, Sanban-cho, Chiyoda-ku		
Tokyo 102, Japan		
Taiwan:	Voice:	+886-2-545-5611
Cheyenne Software, Taiwan Branch	FAX:	Mon-Fri 9 am- 5 pm
Room C, 4th Floor		+886-2-545-5616
170 Tun Hua North Road		
Taipei, Taiwan		

Training

For the convenience of our customers, Cheyenne University has established a network of Authorized Cheyenne Education Centers and Authorized Cheyenne Instructors. For the latest course descriptions and schedules:

- Customers in U.S. / Canada, call: 800-243-9272
- Customers in Europe, Africa, and Middle East, call: +33-1-39-23-18-80
- Customers in Australia, call +61-2-9591944
- Customers in Japan, call: +813-3222-3750
- Customers in Taiwan and Asia, call: +886-2-7951092
- Customers in other areas, call: +1-516-465-4000

CONTENTS

Getting Started

Computer Viruses: An Overview 1-2
About Cheyenne AntiVirus?. 1-3
How does Cheyenne AntiVirus work? 1-4
Cheyenne AntiVirus features 1-5

Protecting Your Windows NT Network

Installing InocuLAN 4.0 for Windows NT. 2-3
Installation 2-3
Protecting your NT Network with the Domain Manager 2-7
Setting up domain-based network protection 2-8
Setting up Real-time protection 2-10
More about Quarantine and Virus Wall: A Test Scenario . 2-15
Scheduling the Domain Scan 2-19
Point-to-Point management 2-25
NetWare Domain Management 2-26
NetWare Domain/Server Security 2-27
Using the NetWare Domain Manager 2-29
Actions and Options for Domain Scans 2-33
Modifying a Scan Job 2-39
Checking the Progress of Your Scan Job 2-41
Checking the Results of Your Scan Job 2-42
Using the Local Scanner. 2-44
Internet-Enabled Download Protection 2-50

Configuring Services, Logs and Broadcasts

The Service Manager 3-3
Configuring InocuLAN's Services. 3-4
Configuring the Event Log 3-6
Configuring the Scan Log. 3-8
Configuring the Virus Directory Purge 3-10
Configuring Broadcast services 3-11

Hands-free configuration 3-11
Protocols 3-13
Time-out Intervals. 3-13
Configuring NT Domains 3-15
Configuring TCP/IP Networks 3-16
Configuring IP Network Masks 3-17
Troubleshooting the InocuLAN network 3-18
Synchronizing broadcast information. 3-19

Automatic Download, Distribution and Update

Automatic Signature Download, Distribution and Update. 4-2
AutoDownload, Distribution and Update: A Scenario 4-5
Updating of Client Workstations 4-21
Updating workstation software. 4-26

Alerting Users When a Virus is Detected

Alert basics 5-2
Running the Alert Manager 5-4
Configuring Alert. 5-6
Editing and creating Port configurations 5-9
Using the Broadcast option. 5-11
Using the Pager option 5-12
Interpreting the numeric pager message 5-14
Using the SNMP option 5-16
Using the Trouble Ticket option. 5-18
Using the E-mail option 5-20
Assigning Attachments to E-mail Messages 5-21
Using the Lotus Notes Option 5-23
Using the CA-Unicenter TNG Option 5-26
Testing the Recipients. 5-31
Alert’s Activity Log 5-32
Alert’s Event Log 5-33
Printing selected objects 5-34

Scanning Your Windows 95 Workstation

About Cheyenne AntiVirus for Windows 95 6-2
Installing AntiVirus for Windows 95 6-3
Installation 6-4
Uninstalling Cheyenne AntiVirus. 6-9
Getting Started with AntiVirus for Windows 95 6-10
Scanning Your Workstation 6-11
Checking the results of your scan 6-16
Windows 95 Enhancement - Local Scanning shell extensions. 6-17
Scanning Mapped Drives 6-18
Using the Windows 95 command line scanner. 6-19
Scheduling a scan job 6-22
Using the DOS command line scanner 6-26

Safeguarding Windows 95 Workstations

Keeping your workstation virus-free 7-3
Using the Real-time-Monitor 7-5
Automatic Loading of the Real-time Monitor 7-5
Configuring the Real-time Monitor 7-7
Using Rescue Disk to protect your critical disk areas 7-14
Creating a Cheyenne AntiVirus Rescue Disk 7-15
What to do if Cheyenne AntiVirus discovers a virus 7-19
Keeping your AntiVirus system up-to-date 7-23
How to use the AutoDownload Manager 7-24
Configuring the AutoDownload Manager 7-26
Configuring FTP Settings 7-28
Configuring Modem Settings 7-29
Scheduled Updates from Windows NT 7-30

Using AntiVirus for Windows

Installing Cheyenne AntiVirus for Windows 8-3
System requirements. 8-3
Configuring your system for installation 8-4
Windows Installation 8-6
Starting Cheyenne AntiVirus 8-15

Using the Quick Access dialog box/toolbar 8-17
Cheyenne AntiVirus virus list. 8-18
Using the Local Scanner 8-20
Options for Workstation Scans 8-23
Checking the Results of Your Scan 8-28
Using the Cheyenne AntiVirus DOS Command Line Scanner 8-30
Keeping your workstation virus-free 8-37
Real-time Monitoring with WIMMUNE 8-39
Protecting your Critical Disk Area 8-41
Using the command line EXAMINE utility 8-46

Using Cheyenne AntiVirus for DOS

DOS Installation 9-3
Starting Cheyenne AntiVirus 9-10
The basic Cheyenne AntiVirus for DOS screens. 9-11
Entering information into fields 9-14
Keys used in Cheyenne AntiVirus for DOS 9-16
Using a mouse with Cheyenne AntiVirus for DOS 9-18
Online help in Cheyenne AntiVirus for DOS. 9-19
Version information 9-20
Temporarily exiting to DOS 9-21
Virus list 9-22
Using the Run Scanner 9-24
Keeping your workstation virus-free 9-30
Using IMMUNE 9-32
Using the EXAMINE Program. 9-37
Protecting your Critical Disk Area 9-42
Command line installation 9-46

Virus Recovery Procedures

What to do if Cheyenne AntiVirus discovers a virus 10-2

Using Cheyenne AntiVirus for Macintosh

About Cheyenne AntiVirus for Macintosh. 11-3

Installing Cheyenne AntiVirus for Macintosh 11-4
Quick Start: Scanning your hard disk for viruses 11-7
About the Cheyenne AntiVirus for Macintosh INIT 11-9
Repairing volumes and folders 11-12
Repairing Individual files 11-15
Repairing floppy disks 11-16
Checking volumes and files 11-18
Repairing or checking AppleShare servers. 11-20
Using the INIT manager 11-21
Saving a log as a text file 11-22

About Computer Viruses

What Is a Computer Virus? A-3

1

Chapter

GETTING STARTED

This chapter explains how to get started using Cheyenne AntiVirus.

In this chapter, you will learn:

Page

1-2 ➢ About viruses

1-3 ➢ About Cheyenne AntiVirus

1-4 ➢ How does AntiVirus work?

1-5 ➢ Cheyenne AntiVirus features

Computer Viruses: An Overview

Similar to a biological virus, a computer virus is a small program that infects *your* computer. The basic characteristics of computer viruses are self-replication and file attachment.

Viruses are not intelligent. They are usually a set of instructional codes to perform a particular function. Some viruses are very complex, like the polymorphic type. This type of virus can replicate itself a bit different each time, so that the newly born viruses are actually a mutant variation of the original.

A virus may be designed to wipe out your CMOS information, reformat your data on the hard drive, or simply replicate itself so many times that you will not be able to access the data that you stored on the computer. Typical viruses are usually very small executable programs that attach themselves to another program. They are usually designed to be stealthy, and destructive.

So why do you need protection from these viruses? A virus, at best, is a nuisance to your system, displaying some obscure texts or graphics on your monitor. In the worst case, a virus destroys valuable data. Thus, to prevent the loss of data or computer down time, you must protect your system against these pesky invaders.

The best protection is prevention. Cheyenne's suite of anti-virus products have all the necessary functions to prevent, detect, and cure viruses using the latest in virus detection technology. In addition, Cheyenne offers monthly virus signature updates to keep your system current to fight against any new viruses.

About Cheyenne AntiVirus?

Cheyenne AntiVirus is an integrated anti-virus solution for your network. Use InocuLAN for Windows NT, *Cheyenne AntiVirus for the Network*, to protect your Windows NT server or workstation. Use Cheyenne AntiVirus desktop versions to protect your workstations running under Windows 95, Windows 3.x, DOS, and Macintosh. InocuLAN is also available for Novell NetWare.

Cheyenne AntiVirus consists of the following products:

Version	Provides virus protection for...
InocuLAN for Windows NT	Your Windows NT server or workstation
Cheyenne AntiVirus for Windows 95	Your Windows 95 machine
Cheyenne AntiVirus for Windows 3.1	Your Windows 3.1 machine
Cheyenne AntiVirus for DOS	Your DOS machine
Cheyenne AntiVirus for Macintosh	Your Macintosh machine

How does Cheyenne AntiVirus work?

Cheyenne AntiVirus scans files on your workstation, using signature checking and a rules-based polymorphic analyzer virus scanner to detect known viruses. In addition, the Cheyenne AntiVirus Real-time Monitor program offers continuous virus protection while you work. Real-time Monitor is a VxD (Virtual Device Driver) that provides native anti-virus protection. VxD programs are more stable and less resource-intensive than TSR-type programs.

If a virus is detected, you decide how the infected file should be handled. You can delete, rename, cure, move, or report an infected file.

Virus prevention methods

Cheyenne uses four basic techniques to detect computer viruses:

- Integrity Checking- determines if the program's contents have changed due to a virus attaching itself to a program. AntiVirus integrity checking primarily is used to check the integrity of the Rescue Disk information.
- Rules-based, Polymorphic Analyzer Detection- observes the way programs behave to detect suspicious program behavior.
- Interrupt Monitoring- observes all program system calls in an attempt to stop the sequence of calls which may indicate virus activities.
- Signature Scanning- method uses a unique set of hexadecimal code, the virus signature, which a virus leaves within an infected file. By searching program files armed with these codes, the signature scanner can detect known viruses. Signature file are updated monthly free of charge. You can download the signature files from our CompuServe (Go Cheyenne), the World Wide Web (www.cheyenne.com), BBS (516-465-3900), and FTP sites worldwide (ftp.cheyenne.com).

Cheyenne AntiVirus features

On the Windows NT platform, InocuLAN's features include:

- Real-time protection provides a hands-free, continuous barrier against viruses that stops infections before they can spread. InocuLAN uses a number of real-time components to protect all avenues of entry into the Windows NT enterprise, including:
- Real-time Scanning Mode: All files going to and from the server are scanned for viruses, including compressed files. With InocuLAN real-time in operation, viruses won't spread through your network.
- Virus Wall: A little-known but very dangerous security leak that many anti-virus products can't stop is the infection of a server by a workstation. InocuLAN stops any infected file from being copied to a server and replacing the clean version of the file, thereby keeping enterprise security intact.
- Virus Quarantine: Users who try to copy infected files to a server are automatically suspended from the machine, isolating the infection before it can spread. A message is sent listing the name of the user who tried to move an infected file.
- Floppy-drive protection: Floppy diskettes are the most common source of virus infections, and InocuLAN fully protects your enterprise from floppy-based viruses. As soon as a floppy diskette is accessed, such as by looking at the disk's contents in My Computer, InocuLAN scans the boot sector, preventing the spread of dangerous boot viruses. When a file is opened or copied from the floppy, InocuLAN scans it before it moves to the hard drive.

- CD-ROM protection: Because you will want to protect your environment from viruses when you download data or access data on CD's, you can now prevent viruses from being copied onto your machine.
- Network drive protection: Another little-understood but common way of spreading viruses happens when files are copied from one mapped drive to another. Even though no file passes through the hard drive of the local machine, InocuLAN will still scan all files moving between mapped drives.
- Internet-enabled: The newest source of virus infections is via the Internet. As users gain nearly limitless access to computers world-wide, the chances of downloading infected files grows exponentially. With InocuLAN running, all file downloads are automatically scanned for viruses *before* they can infect a machine. This includes support for compressed files. InocuLAN works with browsers from both NetScape and Microsoft.
- Groupware Messaging AntiVirus options: More than ever, companies are communicating electronically. As more data is being exchanged, more viruses are spreading by hiding within mail attachments and database files. InocuLAN is the only product that can protect your Lotus Notes or Microsoft Exchange mail systems with its messaging options. Even attached ZIP files are scanned. (Cheyenne is also developing messaging protection for GroupWise, which will be available soon.)
- Support for Windows NT 4.0 includes shell extension integration, providing right-click scanning from any volume, folder, or file.
- Multi-platform support: InocuLAN NT versions for Intel, Digital Alpha, NEC MIPS, and Motorola Power PC.
- Microsoft BackOffice support: InocuLAN NT carries the ***"Designed for BackOffice"*** logo.

- NCSA Certification ensures protection against 100% of the computer viruses in the wild, as certified by the ***National Computer Security Association (NCSA)***.
- New Multiple Source Browser: A new Explorer-like browser makes viewing and selecting servers, directories, and files faster and easier. Multiple sources can be selected for scanning.
- NetWare domain management lets you administer your InocuLAN NetWare servers through the Windows NT console.
- Real-time Copy Cure option makes a copy of the infected file before curing it.
- Automatic Software Download, Distribution and Update: Hands-free downloading and distribution of the latest signature files and search engines using modem or FTP downloads. Supports multi-language, multi-platform networks.
- Point-to-Point Management: InocuLAN Servers can be managed by entering the machine name. This mean InocuLAN can communicate with all InocuLAN servers, even across segmented LANS where broadcasts are filtered out.
- Compressed Files: We currently support scanning compressed files and internet downloads in.ZIP,.ARJ, LHA, LZH, MIME, UUEncoded, and Microsoft compressed formats.
- Scheduled Scanning allows administrators to scan networked servers at scheduled time intervals.
- Domain Support allows administrators to configure servers into InocuLAN domains. Multiple servers can be configured at one time.
- Updated Alert System immediately notifies selected users of a virus threat through network broadcast, print queue/trouble ticket, Microsoft Mail, Microsoft Exchange, SNMP, and pager.
- Remote System Event Log Support uses Alert 4.0 to forward Alarm information to remote server’s system event logs.

- Flexible Reporting includes scanning results, virus incidents, configuration changes, and status reports. Reports are completely automated and centralized across InocuLAN domains.

On Windows 95 and other platforms, Cheyenne AntiVirus features include:

- Windows 95 32-bit capability takes full advantage of the enhanced speed and power available in Windows 95.
- Windows 95 Graphical User Interface provides point-and-click functionality, making tasks easier and encouraging end-user implementation.
- Local Scanner scans local drives, mapped drives, and floppy disks for viruses.
- The Real-time Monitor program detects viral behavior of known and unknown viruses. It scans files as they are about to be executed or accessed, and examines RAM for viruses, and also provides the user with pop-up messages when a virus is detected. Real-time Monitor scans files for viruses on an incoming and outgoing basis as files move to and from networked computers. This prevents viruses from spreading. From the Real-time Monitor icon, you can also manage (enable and disable) the Real-time Monitor program.
- Scheduled Scanning allows you to run virus scans at pre-determined intervals.
- Native protection is provided by the Real-time Monitor, which is a VxD (Virtual Device Driver) program.
- Shell Extension provides a quick way to scan a workstation, mapped drive or floppy disk without starting the Cheyenne AntiVirus program. It can be launched with a few mouse clicks from the Windows 95 Explorer.
- Rescue Disk protection checks the CMOS RAM information, master boot sector, operating system boot sector, partition table, I/O system file, shell file and Windows 95 (or Windows or DOS)

system files. This critical disk area is backed up by Cheyenne AntiVirus and can be restored in case of infection or corruption.

- ➢ EXAMINE verifies the integrity of your workstation Rescue Disk during the boot process. The boot sector is examined before your operating system begins to load.
- ➢ DOS command line scanner lets you automate scanning at start up time through simple AUTOEXEC.BAT commands.
- ➢ Virus signature updates, available online from Cheyenne, keep you protected from the latest viral threats to your system.

2

Chapter

PROTECTING YOUR WINDOWS NT NETWORK

This chapter explains how to scan and safeguard your Windows NT network.

In this chapter, you will learn:

Page		
2-3	➢	How to install InocuLAN 4.0 for Windows NT client
2-8	➢	How to Setup Domain-based Network Protection
2-10	➢	How to Setup Real-time Protection
2-15	➢	About Quarantine and Virus Wall
2-26	➢	NetWare Domain Management
2-29	➢	Using the Domain Scanner
2-44	➢	How to use the Local Scanner

2-50 ➢ About Internet Virus Protection

Installing InocuLAN 4.0 for Windows NT

System requirements

To install and use InocuLAN 4 and Alert on your Windows NT computer, the following hardware and software requirements must be satisfied:

Machine Type	80486 DX or higher PC, Alpha, MIPS or Power PC.
Operating System	Windows NT version 3.51 or higher
Minimum System Memory	16 Megabytes minimum, 32 megabytes recommended
Disk Space	8 Megabytes

Installation

NOTE:Please read the Release Notes fully before installing.

To install InocuLAN 4.0 for Windows NT:

1. Insert the InocuLAN Installation CD-ROM into the CD-ROM drive.

2. Choose Run from the File Menu in the Windows NT Program Manager. On Windows NT version 4.0, click on the Start button and select Run.

   The Run dialog box opens.

3. In the Run dialog box, type **`D:CDSETUP`** (This is assuming that your drive D is the CD-Rom drive) and then click OK.

4. The InocuLAN Welcome screen will appear, listing the system requirements. Click Next to continue.

5. The License screen appears.

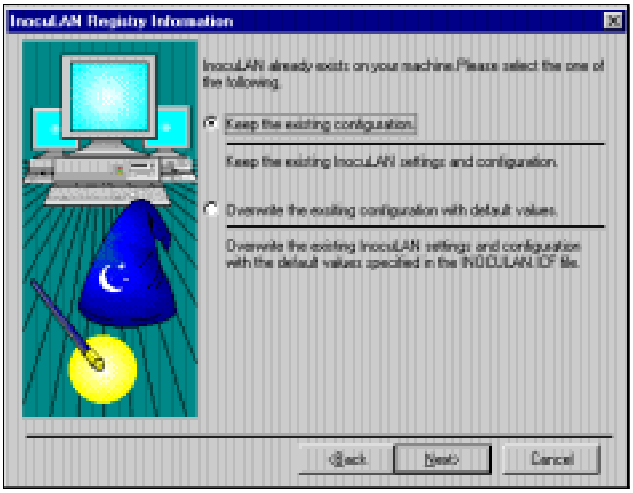
If you are using a CD Key for licensing, enter the key in the appropriate spaces. If you are using a license file, direct InocuLAN to the file's location using the Browse button.

Click on Next to continue.

6. The User Information screen appears. Enter your name and company information on the screen and click on Next to continue.

7. If you have a previous version of InocuLAN on the machine, the Registry Information screen will appear:

.



InocuLAN already exists on your machine.Please select the one of the following.

● Keep the existing configuration.

Keep the existing InocuLAN settings and configuration.

○ Overwrite the existing configuration with default values.

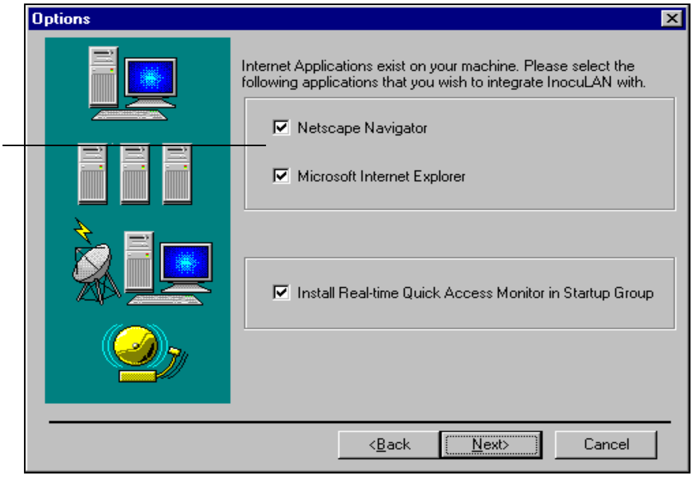
Overwrite the existing InocuLAN settings and configuration with the default values specified in the INOCULAN.ICF file.

If you wish to keep your previous InocuLAN information, such as scan logs and domain configurations, choose *Keep the existing configuration.*

To overwrite previous information, select *Overwrite the existing configuration with default values*. This sets all values to the InocuLAN default settings.

Click on Next to continue.

8. The InocuLAN Options screen appears:



Internet Applications exist on your machine. Please select the following applications that you wish to integrate InocuLAN with.

☑ Netscape Navigator

☑ Microsoft Internet Explorer

☑ Install Real-time Quick Access Monitor in Startup Group

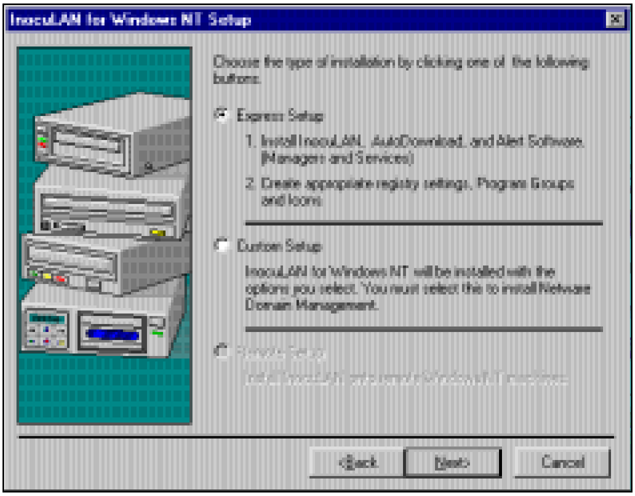
These fields will be grayed out if you do not have an applicable browser on your machine.

InocuLAN provides automatic scanning of internet downloads. To install the internet helper applications, select the applicable browser(s).

The Real-time Monitor can be accessed from the Windows NT 4.0 system tray via the Quick Access Monitor. If you would like the Quick Access Monitor to appear on startup, select the installation option.

Click on *Next* to continue.

9. Choose either Express Setup or Custom setup.



Choose the type of installation by clicking one of the following buttons.

● Express Setup

1. Install InocuLAN, AutoDownload, and Alert Software. (Managers and Services)
2. Create appropriate registry settings, Program Groups and Icons.

○ Custom Setup

InocuLAN for Windows NT will be installed with the options you select. You must select this to install Netware Domain Management.

○ Remote Setup

Install InocuLAN onto remote Windows NT machines

Express setup will install all major InocuLAN components. Custom Setup will allow you to choose from the following:

- Install all Alert files.
- Install AutoDownload (Server and Manager).
- Install InocuLAN for Windows NT Manager
- Install InocuLAN for Windows NT Server.
- Install NetWare Domain Manager

NOTE: The only way to install NetWare Domain Management is through Custom Setup.

Click on Next to continue.

10. The Select Directory screen appears. Click on Next to accept the default values, or enter a new directory and path.

11. A message screen will note that all necessary information has been collected. At this point, you may still click the Back button to change your installation settings.

    Click *Finish* to begin the product installation.

12. InocuLAN will begin copying files to your hard drive. You will be prompted when the installation is complete. Restart your InocuLAN machine for all settings to take effect.

Protecting your NT Network with the Domain Manager

The Domain Manager lets you group servers into logical units called InocuLAN Domains. Server management can be done at the domain level, so information entered once applies to all servers in the domain. Servers can also be managed individually within a domain.

There are several steps you can take to ensure network protection. The steps are as follows:

- ➢ Group your NT machines into InocuLAN domains.
- ➢ Configure and start up InocuLAN's Real-time Monitor for each domain. This will immediately protect your network from new virus infections.
- ➢ Scan the entire network to locate any viruses that may have infected your machines before real-time monitoring was turned on.
- ➢ Schedule full domain scans to run at a regular interval. While InocuLAN's multiple real-time capabilities effectively stop new virus infections, there are two reasons you should also run a scheduled scan.

If for any reason real-time monitoring is turned off on a particular machine, that machine is vulnerable to infection until the monitor is turned back on. A periodic scan of the machine will locate any viruses that may have infected the machine while real-time was shut down.

New viruses are always being created. Cheyenne Software provides monthly virus signature file updates to locate the latest virus threats. It is possible that a new virus can infect your machine before the latest signature file is available. Running a domain scan as soon as a new signature file is available ensures that new viruses are detected as soon as possible.

- ➢ Set up InocuLAN's automatic file download and distribution system, to keep your InocuLAN network up-to-date.

Setting up domain-based network protection

The following pages will explain how to set up an InocuLAN domain, start and configure real-time virus protection, and scan your network servers. In our example, we will show how to create and manage an InocuLAN domain of five Windows NT servers.

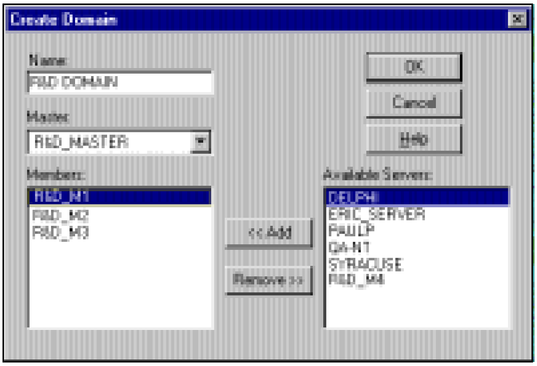
Creating the domain

The first step is to set up the InocuLAN domain.

1. Open the Domain Manager.

2. Click the Create Domain button.

   The Create Domain window will show you which servers are available to place into a domain. A machine must have InocuLAN installed to be seen in the Available Servers list.



Create Domain

Name: R&D DOMAIN

Master: R&D_MASTER

Members:
R&D_M1
R&D_M2
R&D_M3

Available Servers:
DELPHI
ERIC_SERVER
PAULP
QA-NT
SYRACUSE
R&D_M4

3. In this example, we will create an InocuLAN domain called R&D DOMAIN. Enter this name in the Name field.

4. Each InocuLAN domain requires a master server. The master server sends management information to all other member servers in the domain. Any available server can become the master server. Select your master server using the drop-down list in the Master field. For our example, we have selected R&D_MASTER.

   Picking the master server: There are 3 factors to consider when choosing a master server.

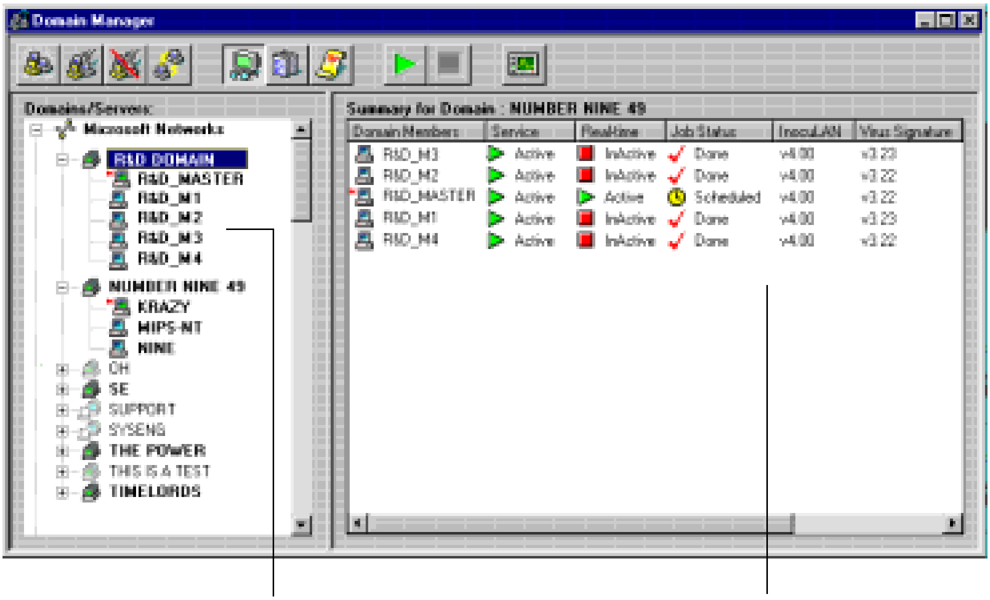
In a mixed environment of InocuLAN versions 1.01 and 4, the master server *must* be an InocuLAN 4 machine.

The master server will contain scanning logs for all machines in the domain. The log will grow over time, so you shouldn't pick a machine that is very short of disk space.

The master server will collect Alerts from its members and send them out via the Alert manager. If you wish to use paging, you must select a server that has a modem.

5. Add member servers to the domain by highlighting them in the Available Servers field and clicking Add. In our example, we are adding four other servers into the domain, creating a total InocuLAN domain consisting of five Windows NT machines.

   Upon completion, R&D DOMAIN and all the member servers will be seen in the Domain Manager window.



Summary for Domain : NUMBER NINE 49

Domain Members	Service	RealTime	Job Status	InocuLAN	Virus Signature
R&D_M3	Active	InActive	✓ Done	v4.00	v3.23
R&D_M2	Active	InActive	✓ Done	v4.00	v3.22
R&D_MASTER	Active	Active	Scheduled	v4.00	v3.22
R&D_M1	Active	InActive	✓ Done	v4.00	v3.23
R&D_M4	Active	InActive	✓ Done	v4.00	v3.22

The newly created InocuLAN domain is shown here.

Information about machines in the domain is shown in the Summary window. If you click on a machine within the domain, you will see additional details about that machine.

Setting up Real-time protection

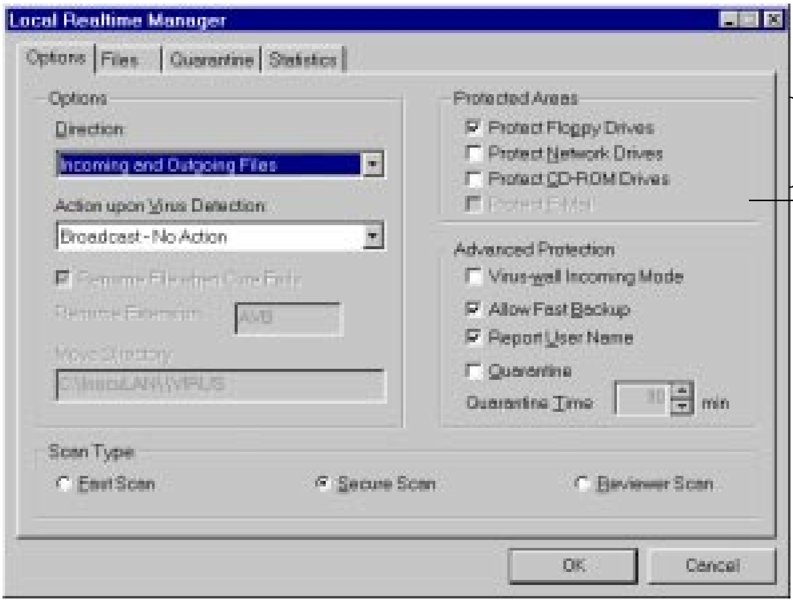
Now that five servers have been logically grouped into R&D DOMAIN, we want to immediately protect them from viruses by configuring real-time protection.

Configuring the Real-time Monitor

1. Highlight R&D DOMAIN in the Domains/Servers window.

2. Click the Real-time Monitor button.

   The Real-time Monitor Options window appears:



Options

Direction: Incoming and Outgoing Files

Action upon Virus Detection: Broadcast - No Action

☑ Rename File when Cure Fails

Rename Extension: AVB

Move Directory: C:\InocuLAN\VIRUS

Protected Areas

☑ Protect Floppy Drives
□ Protect Network Drives
□ Protect CD-ROM Drives
☑ Protect E-Mail

Advanced Protection

□ Virus-wall Incoming Mode
☑ Allow Fast Backup
☑ Report User Name
□ Quarantine

Quarantine Time: 30 min

Scan Type

○ Fast Scan ● Secure Scan ○ Reviewer Scan

Protect your floppy, Network, and CD-ROM Drives.

Email scanning options are seen only if the email Antivirus Option is installed.

3. In the Direction field, select Incoming and Outgoing Files.

   Files being copied *to* the server and files being opened for writing on the server are *incoming*. Incoming files are scanned after the file is closed.

   Files being copied *from* the server and files that are being executed from the server are *outgoing*. Outgoing files are scanned when the file is opened. If the file is found to be infected, you will be denied access to it.

Other setting choices are *Incoming Files, Outgoing Files*, or *Disable*.

Scanning action

4. You control what happens to an infected file in the Action Upon Virus Detection field.
   - Because you want to decide whether or not a file is cured on an individual basis, you choose the *Broadcast - No Action* option.
   - If you prefer that an infected file be deleted automatically, choose *Delete File*.
   - *Copy and Cure* makes a copy of the infected file and moves it to the INOCULAN/VIRUS directory before curing the file. InocuLAN removes viruses from infected files and restores the files to their original state. If the file cannot be cured, it is renamed with an AVB extension (refer to 'Rename File' below). <u>Even if InocuLAN cures the file, we recommend you delete the infected file and then restore the original file from a backup or the product installation disks</u>.
   - *Rename File* renames infected files by giving them an AVB extension. AVB files will not be scanned by InocuLAN. Infected files with the same name will be given incremental extensions in the form AV#, for example: FILE.AV0, FILE.AV1, etc.
   - *Move File* moves an infected file from its current directory to the INOCULAN\VIRUS directory.
   - *Purge File* deletes an infected file so that it cannot be recovered.
   - *Rename and Move File* renames infected files by giving them an AVB extension and then moving them to the INOCULAN\VIRUS directory.

Whenever an action is taken, InocuLAN sends messages via Broadcast, Microsoft Mail, Microsoft Exchange, SNMP, Trouble Ticket, and Pager, if they have been set up in Alert.

The message also appears in the Scanning Log and the Windows NT Event Log.

Scan Type

5. The level of scanning is set in the Scan Type field.

   Because you want files to be scanned completely, choose *Secure Scan. Fast Scan,* which runs more quickly than Secure Scan, checks only the beginning and end of each data file, the place where a virus is most likely to hide. Fast Scan improves scanning efficiency when processing large groups of data files, *but it is possible for a file to have a virus that is be missed by Fast Scan*.

   If you suspect you have a virus but Secure Scan is not detecting one, you can use the *Reviewer Scan* option. The Reviewer Scan can also detect viruses that are inactive or have been deliberately modified, such as in a virus testing laboratory. Note that in unique circumstances, Reviewer Scan can generate a false alarm. Therefore, if you are using Reviewer Scan as your standard scanning option, you should use the Report Only option.

Floppy disk protection

6. Because floppy diskettes are the most common source of virus infections, we want to protect R&D DOMAIN from infected diskettes. Under Protected Areas, click Protect Floppy Drives.

   As soon as a floppy diskette is accessed on any of the domain machines, InocuLAN scans the boot sector, preventing the spread of dangerous boot viruses. When a file is opened or copied from the floppy, InocuLAN scans it before it moves to the hard drive.

CD-ROM Protection

7. Because you will want to protect your environment from viruses when you download data or access data on CD’s, you can now prevent viruses from being copied onto your machine.

   Click on Protect CD-ROM Drive to enable this feature.

Server-to-Server protection

8. The users of R&D DOMAIN often copy files from one server to another.

   By selecting *Protect Network Drives,* InocuLAN will scan all files moving between mapped drives, even if no file passes through the hard drive of the local machine.

Allow Fast Backup

9. The servers in R&D DOMAIN are backed up to tape each night.

   Normally, the Real-time Monitor would scan each file as it was being copied to tape, thereby slowing the backup. However, since you scan the servers before the backup, you don't want to repeat the scanning during the backup. Click *Allow Fast Backup* to copy files to tape without virus scanning. InocuLAN will only skip files being opened by backup software. (Note that Cheyenne's ARCserve backup product integrates intelligently with InocuLAN, resulting in far less performance degradation than other backup products.)

Virus Wall

10. R&D DOMAIN supports hundreds of users.

    Not all of them have anti-virus protection on their workstations, and some that do turn it off. This creates a very dangerous hole in your network security: infected files can be copied from a workstation to a server. By selecting *Virus-wall Incoming Mode*, InocuLAN will stop any infected file from being copied to a server and replacing the clean version of the file, thereby keeping enterprise security intact.

NOTE: InocuLAN currently protects .EXE, .COM, .DOC, .DOT, and .XLS files of less than 2MB in size for performance reasons.

Virus Source Tracking

11. It is important for the administrator to know who has tried to copy an infected file to R&D DOMAIN.

    When *Report User Name* is selected, InocuLAN will report the name of the user trying to pass the virus. That person can then be contacted, and the virus deleted from their local machine.

Virus Quarantine

12. Because no network is perfect, and because end-users behave unpredictably, InocuLAN provides an exceptional level of protection through its virus Quarantine capability.

    If Quarantine is activated, a user who attempts to move an infected file onto a server, or to execute an infected file at the server console, will be blocked from any further access to the server for the length of time stipulated in the *Quarantine Time* field. Quarantine ensures that the virus doesn't have a chance to spread before the infected workstation can be cleaned.

The names of quarantined users are found under the Quarantine tab in the Real-time Monitor Options screen. The administrator can grant the quarantined users access again by removing their name from the Quarantine screen.

NOTE:The Administrator account on the Windows NT machine cannot be quarantined. However, users with administrator rights can and will be quarantined.

Selecting files to scan

12. Now that the scanning options are set, you have to select the types of files you will scan.

    Click on the Files tab.

13. Choose Scan Compressed File for InocuLAN to scan compressed files.

    By default, InocuLAN scans files of the ZIP and ARJ format, as well as LHA, LZH, MIME, UUEncoded, and Microsoft compressed files. These files end with an underscore, such as: START.EX_. To add other file types, click the Add button.

14. Click OK for your all options to take effect. Real-time scanning begins immediately.

With all of InocuLAN's Real-time scanning options now enabled, the R&D DOMAIN servers are thoroughly protected from all new viruses entering the network.

However, there may have been viruses present on the network before InocuLAN's Real-time scanning was turned on. To ensure that the network is clean, a full domain scan should be run. Instructions for doing so follow.

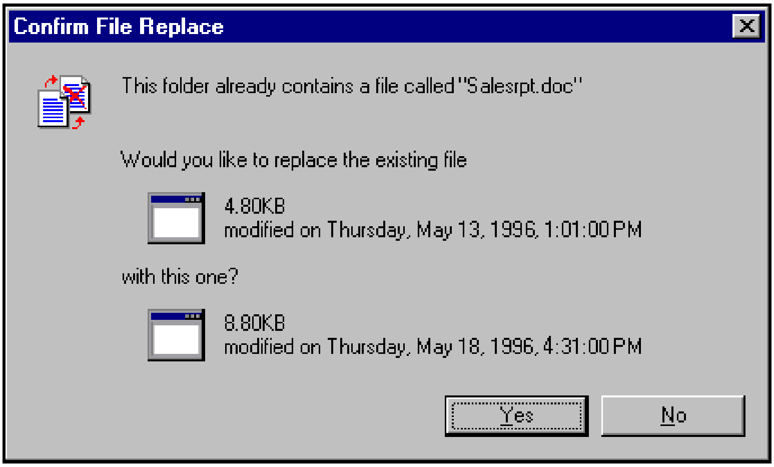
More about Quarantine and Virus Wall: A Test Scenario

To better understand the unique capabilities of the Quarantine and Virus Wall options, we will illustrate a test example.

In this scenario, we assume that user PeterE copied the file SALESRPT.DOC from the server to work with the file. Unfortunately, PeterE never scans his workstation for viruses, even though he has an anti-virus program. This resulted in the SALESRPT.DOC file becoming infected. PeterE will now attempt to copy the newly infected file back to the server. In an enterprise that didn't have InocuLAN's unique protection, the original SALESRPT.DOC file would be replaced with the infected version. Now the virus would be on the server, and the important data in SALESRPT.DOC would be at risk. Even worse, many people work with SALESRPT.DOC, so within a week dozens of people might have the virus.

A recipe for enterprise disaster?   Not if InocuLAN is up and running. Following are actual screens shots of this test scenario.

1. First, PeterE starts to copy the file back to the server. His machine asks him if he would like to replace the current file with the new version. Of course, he answers Yes. Without InocuLAN, the damage would already be done.



Confirm File Replace

This folder already contains a file called "Salesrpt.doc"

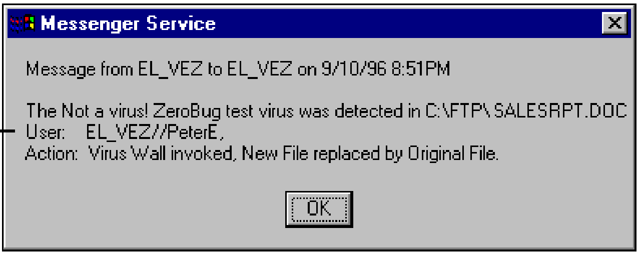
Would you like to replace the existing file

4.80KB
modified on Thursday, May 13, 1996, 1:01:00 PM

with this one?

8.80KB
modified on Thursday, May 18, 1996, 4:31:00 PM

2. Fortunately, InocuLAN is running. Within seconds, the following appears on the NT Server:



Message from EL_VEZ to EL_VEZ on 9/10/96 8:51PM

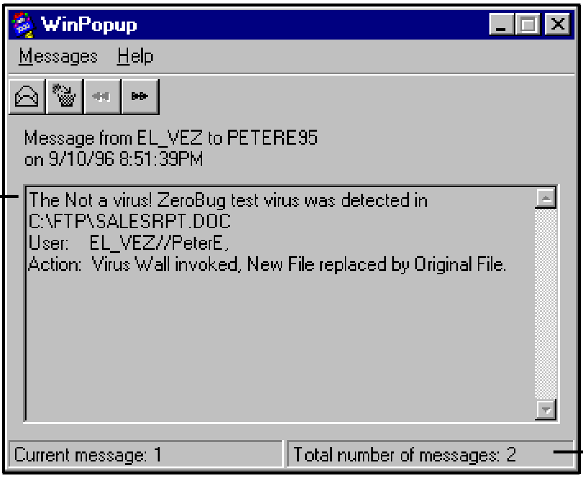
The Not a virus! ZeroBug test virus was detected in C:\FTP\ SALESRPT.DOC
User: EL_VEZ//PeterE,
Action: Virus Wall invoked, New File replaced by Original File.

The administrator clearly sees who is trying to send a virus.

➢ Virus Wall stops the infected file from overwriting the good file, and the important data in SALESRPT.DOC is safe, as is the server.

3. Meanwhile, on PeterE’s machine, the following appears:

➢



Message from EL_VEZ to PETERE95
on 9/10/96 8:51:39PM

The Not a virus! ZeroBug test virus was detected in
C:\FTP\SALESRPT.DOC
User: EL_VEZ//PeterE,
Action: Virus Wall invoked, New File replaced by Original File.

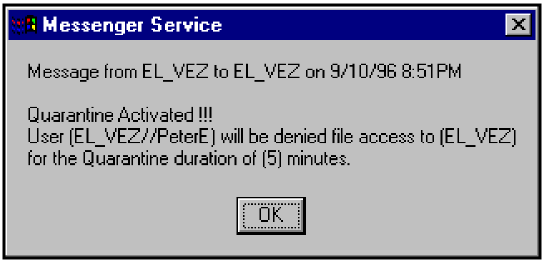
Current message: 1
Total number of messages: 2

PeterE is informed that a virus was in his file, and that the Virus Wall has protected the server.

WinPopup shows a second message is waiting.

To receive messages from the NT server, the Windows 95 machine is running WinPopup. To run WinPopup, open the Run box and enter `Winpopup`. You may want to add Winpopup to your Startup group if you are using Quarantine. (Winpopup will also work on Windows 3.x workstations.)

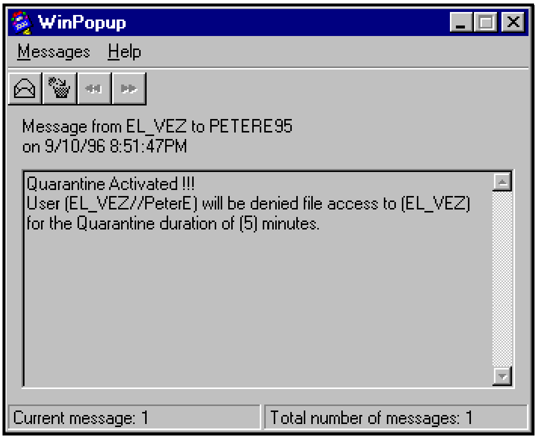
4. After the administrator clicks OK on the first message, a second informs him that PeterE will be blocked from the EL_VEZ server for five minutes:



Message from EL_VEZ to EL_VEZ on 9/10/96 8:51PM

Quarantine Activated !!!
User (EL_VEZ//PeterE) will be denied file access to (EL_VEZ)
for the Quarantine duration of (5) minutes.

5. At the same time, when PeterE reads his second WinPopup message, he learns that he has been quarantined for five minutes.



Message from EL_VEZ to PETERE95
on 9/10/96 8:51:47PM

Quarantine Activated !!!
User (EL_VEZ//PeterE) will be denied file access to (EL_VEZ)
for the Quarantine duration of (5) minutes.

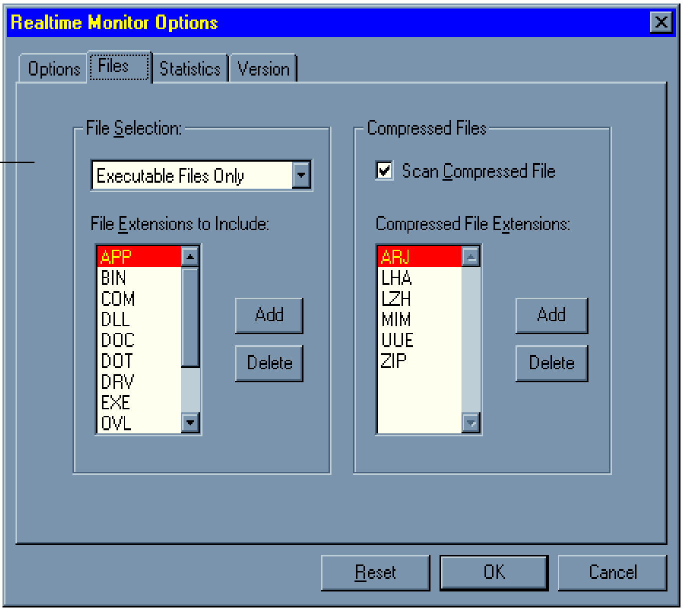
Current message: 1

Total number of messages: 1

The end result? The administrator knows that PeterE has a virus on his machine, and he can take action to remove it. PeterE knows that he has a virus, and he knows precisely how long he will be blocked from the server. And most importantly, the server has not been infected, and the original SALESRPT.DOC file is safe. The enterprise is secure.

Important! Because Quarantine blocks server access based on user name, any user named PeterE would have been quarantined in the above scenario. This is particularly important if a network has many people sharing the same user name, such as GUEST. All users names GUEST would be quarantined if one user tried to copy an infected file.

InocuLAN can scan all files, or you can include or exclude selected file types. You can also add and/or delete file types from the default list.



File Selection: Executable Files Only

File Extensions to Include: APP, BIN, COM, DLL, DOC, DOT, DRV, EXE, OVL

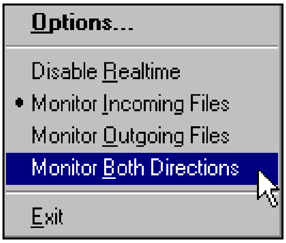
Compressed Files

☑ Scan Compressed File

Compressed File Extensions: ARJ, LHA, LZH, MIM, UUE, ZIP

Windows NT 4.0 Enhancement - Real-time Quick Access Monitor

If you are using Windows NT 4.0, you can access the Real-time Monitor through the system tray. If you chose to install the Quick Access Monitor during setup, the icon will automatically appear in the system tray. To start it manually, click the Start button, then Programs, InocuLAN for Windows NT, and InocuLAN Real-time Monitor.



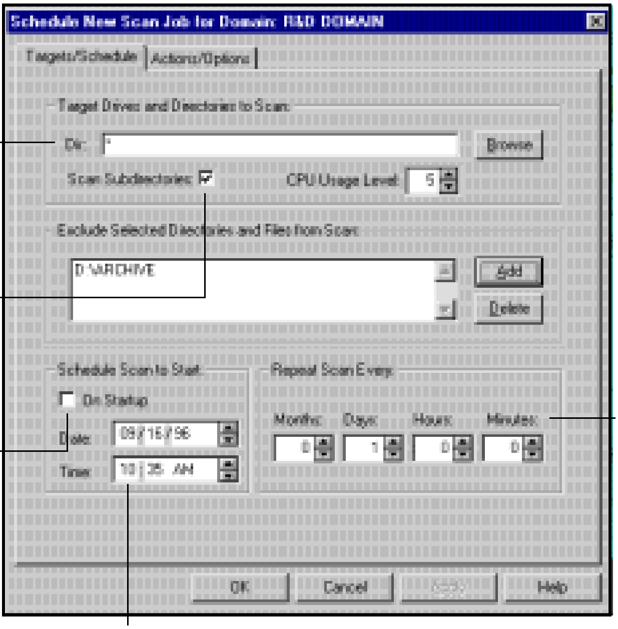
Double-clicking on the Quick Access Monitor icon (at right) will open the Real-time Monitor's Options screen. Right-clicking on it will also allow you to open the Options screen, alter the direction of files being scanned or disable the monitor, as shown at left.

Scheduling the Domain Scan

With the domain set up and real-time scanning in place, the next task is to schedule a domain scan job.

1. Click the Add/Re-Schedule a Scan Job button.

   Information about what and when to scan is entered on the Targets/Schedules tab:



Schedule New Scan Job for Domain: R&D DOMAIN
Targets/Schedule
Actions/Options
Target Drives and Directories to Scan
Browse
Exclude Selected Directories and Files from Scan
Add
Delete
Schedule Scan to Start
Repeat Scan Every
OK
Cancel
Apply
Help

Dir: *

Scan Subdirectories: ☑

CPU Usage Level: 5

D:\ARCHIVE

□ On Startup

Date: 09/16/96

Time: 10:35 AM

Months: 0 Days: 1 Hours: 0 Minutes: 0

The asterisk '*' indicates that all drives will be scanned. To scan only selected drives, click the Browse button and choose the drives you want to scan.

Check here to scan all subdirectories beneath the source drive.

You can scan your InocuLAN machines as they start up by clicking here. This will insure a clean machine before work starts.

Indicate when the scan should start. The default is the current date and time.

To run a scan at regular intervals, set the repeat time here. Leave at zero to scan only once. This shows a scan set to run every day.

2. Because the servers on the R&D DOMAIN are heavily used, you don't want the scanning process to utilize too much CPU power.

   Set the *CPU Usage Level* to a relatively low level, such as 3. A less busy domain could be set at a higher level, up to 10, which gives full CPU power to the scanning engine. This value is best determined through usage.

3. One directory in the domain, D:\ARCHIVE, contains a large number of compressed archive files.

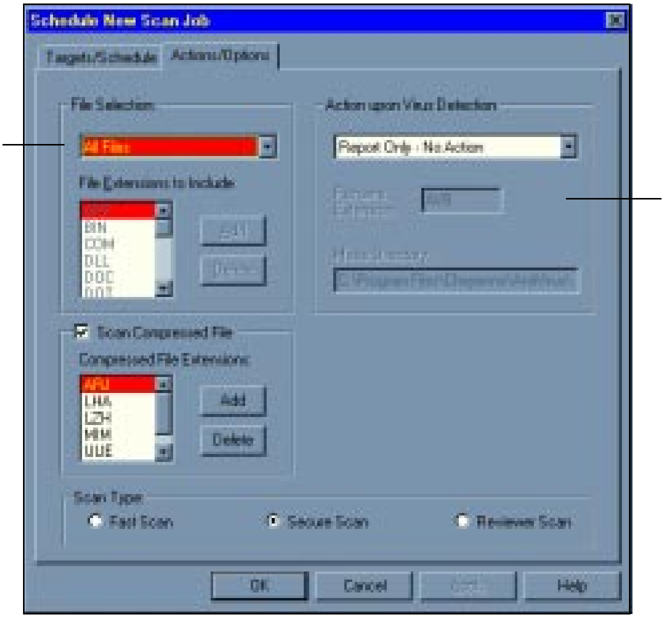
This directory takes a long time to scan. However, since all your archive files are scanned before being compressed, you know they are virus-free.

You can skip this directory by adding it to the *Exclude Selected Directories and Files from Scan* field.

Setting scan actions and options

4. Now you must select which scanning options to use, and what to do if a virus is found.

   Click the Action/Options tab on the Schedule New Scan Job screen.



Schedule New Scan Job

Targets/Schedule | Actions/Options

File Selection: All Files

File Extensions to Include: BIN, COM, DLL, DOC, DOT

☑ Scan Compressed File

Compressed File Extensions: ARJ, LHA, LZH, MIM, UUE

Action upon Virus Detection: Report Only - No Action

Scan Type: ○ Fast Scan ● Secure Scan ○ Reviewer Scan

InocuLAN can scan all files, or you can include or exclude selected file types. You can also add and/or delete file types from the default list.

Rename of the file extension(s) will occur if Cure fails

5. Select the options you want to include with the scanning job.

   Choose *Scan Compressed File* for InocuLAN to scan compressed files.

   By default, InocuLAN scans files of the ZIP and ARJ format, as well as LHA, LZH, MIME, UUEncoded, and Microsoft compressed files. These files end with an underscore, such as: START.EX_. To add other file types, click the add button.

Scanning action

6. You control what happens to an infected file in the Action Upon Virus Detection field.

   - Because you want to decide whether or not a file is cured on an individual basis, you choose the *Broadcast - No Action* option.
   - If you prefer that an infected file be deleted automatically, choose *Delete File*.

- *Cure Files* removes viruses from infected files and restores the files to their original state. If the file cannot be cured, it will be renamed with an AVB extension (refer to 'Rename File' below). Even if InocuLAN cures the file, we recommend you delete the infected file and then restore the original file from a backup or the product installation disks.
- *Rename File* renames infected files by giving them an AVB extension. AVB files will not be scanned by InocuLAN. Infected files with the same name will be given incremental extensions in the form AV#, for example: FILE.AV0, FILE.AV1, etc.
- *Move File* moves an infected file from its current directory to the INOCULAN\VIRUS directory.
- *Purge File* deletes an infected file so that it cannot be recovered.
- *Rename and Move File* renames infected files by giving them an AVB extension and then moving them to the INOCULAN\VIRUS directory.

Whenever an action is taken, InocuLAN sends messages via Broadcast, Microsoft Mail, Microsoft Exchange, SNMP, Trouble Ticket, and Pager, if they have been set up in Alert. The message also appears in the Scanning Log and the Windows NT Event Log.

Scan Type

7. The level of scanning is set in the Scan Type field.

Because you want to ensure that files are scanned in their entirety, you choose *Secure Scan*. *Fast Scan*, which will run quicker than Secure Scan, checks only the beginning and end of each data file, the place where a virus is most likely to hide. Fast Scan will improve scanning efficiency when processing large groups of data files, *but it is possible for a file to have a virus that will be missed by Fast Scan*.

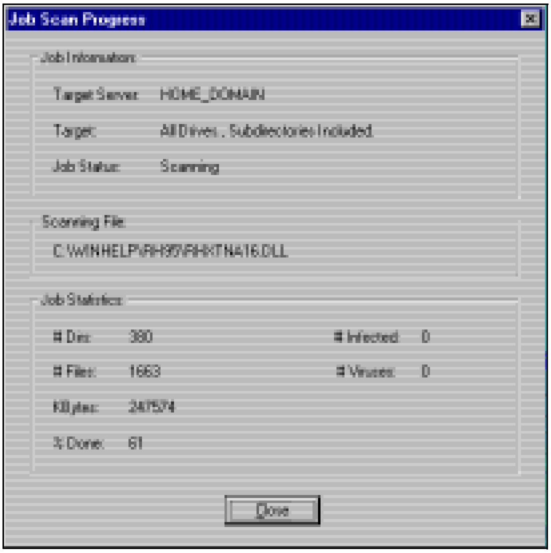
If you suspect you have a virus but Secure Scan is not detecting one, you can use the *Reviewer Scan* option. The Reviewer Scan can also detect viruses that are inactive or have been deliberately modified, such as in a virus testing laboratory. Note that in unique circumstances, Reviewer Scan can generate a false alarm. Therefore, if you are using Reviewer Scan as your standard scanning option, you should use the Report Only option.

8. Click OK to apply your domain scanning settings.

Starting the domain scan and checking scan progress

After clicking OK on the Schedule New Scan Job screen, the scan is set to start based on your configuration. The *Job Status* field in the Domain Manager window will tell you if a job is scheduled to begin, if it is currently scanning, or if the scan has completed.

If a scan is shown as *Active*, you can view the scan progress by clicking on that job to bring up the Scan Progress window:



Target Server: HOME_DOMAIN
Target: All Drives , Subdirectories Included
Job Status: Scanning

C:\WINHELP\RH97\RHXTNA16.DLL

Dirs: 380
Infected: 0
Files: 1663
Viruses: 0
KBytes: 247574
% Done: 61

The progress of the scan job is dynamically displayed in the window, along with an indication of how much of the scan has completed.

NOTE: You should not leave the Scan Progress window open for the length of the scan because it will slow down the scanning operation.

Viewing the scan results

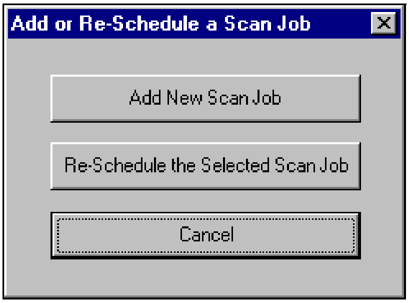
After your scan job is complete, you can view the results of your scan as follows:

1. Highlight a domain and click the Scan Job and Log View icon.
2. In the Job Log window, double-click a log to access the scanning record information.

Modifying a Scan Job

Once you have scheduled a new scan job, it can be modified to fit your changing requirements.

1. Highlight the scheduled job in the Job Queue Screen.
2. Click the Add/Re-Schedule a Scan Job button.
3. The Add or Re-schedule a Scan Job screen is displayed:


Add or Re-Schedule a Scan Job
Add New Scan Job
Re-Schedule the Selected Scan Job
Cancel

4. Click the Re-Schedule the Selected scan job button.

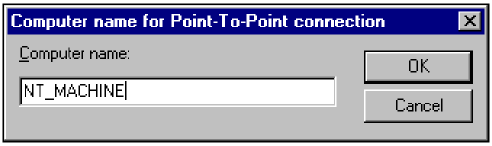
   The Modify/re-schedule Scan Job dialog box opens.
5. Make the changes in either the Targets/Schedule screen or the Actions/Options screen.
6. Click OK when done to apply the changes.

Point-to-Point management

InocuLAN servers periodically send broadcasts, allowing the InocuLAN browser to locate them. However, your network may be configured to filter such messages, and some InocuLAN machines may not appear in the browser. If this is the case, you can attach to those machines directly using point-to-point management.

To configure Point-To-Point management:

1. Click the Point -To- Point button in the Domain Manager window. This will open the computer name entry window:



Computer name for Point-To-Point connection

Computer name: NT_MACHINE

2. Enter the name of the InocuLAN server and click OK.

   The server appears in the browser under the Point-to-Point heading.

NOTE: Machines located by point-to-point management cannot be included as part of an InocuLAN domain and must be administered separately.

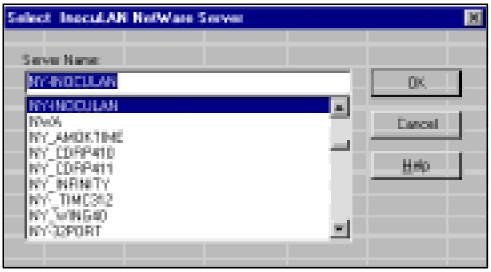
NetWare Domain Management

InocuLAN 4 for Windows NT gives you the ability to manage your InocuLAN for NetWare domains through the Windows NT console.

To manage your InocuLAN for NetWare domains:

1. Click on the Domain Manager for NetWare button in the Quick Access screen.

2. The Select InocuLAN NetWare Server screen appears. All available NetWare servers show in the list. Choose any server that has InocuLAN for NetWare running on it.



Server Name: NY-INOCULAN

NY-INOCULAN
NWA
NY_AMOKTIME
NY_CORP410
NY_CORP411
NY_INFINITY
NY_TIMC312
NY_WING40
NY-32PORT

Click on OK to continue.

3. The InocuLAN for NetWare Domain Manager will appear.

NetWare Domain/Server Security

Cheyenne AntiVirus protects your domains and servers from unauthorized access by requesting a name and password the first time an Cheyenne AntiVirus domain or server is accessed. The password requested may be an user ID or a supervisor ID, depending on the requested action. You are granted read-only right regardless of what user ID you login as. If you want to change a setting or submit a scan job, you must login to the Cheyenne AntiVirus server or domain with an user ID that has supervisor rights. The user ID and the password are automatically kept by the Cheyenne AntiVirus program. Thus, you are only prompt for an ID and password when Cheyenne AntiVirus needs to validate your rights on a particular server. With a NDS login, you will also need Administrator rights on the Cheyenne AntiVirus server to perform any modifications to the system.

For example:

There are four servers: S1 (Bindery), S2 (Bindery), S3 (NDS), S4 (NDS) with Cheyenne AntiVirus installed. There are two Administrators and one end user. The end user has only read rights to monitor the three servers. The first Admin has root Admin rights, thus he/she can change and submit scan job on all three servers. If the first Admin have different ID and password for all four servers, he/she is prompted for a security validation all four times for the four servers. The second Admin only has supervisor rights to the two Bindery servers. Because the second Admin has kept the same user ID and password on both S1 and S2, he/she is prompted only once to administrate the two servers. And if the second Admin tries to manage S3 or S4, he/she is granted read-only rights.

After selecting the Domain Manager option, the Domain Manager window opens showing all available Cheyenne AntiVirus domains and single-servers. When you attempt to perform an action, such as scheduling a scan job, you must select an available Cheyenne AntiVirus server, and a security window requests for a username and password.

After entering the correct information, you can perform all Cheyenne AntiVirus functions for as long as the Cheyenne AntiVirus Manager remains open. If you close the Cheyenne AntiVirus manager and re-open it at a later time, you are again asked for a password. Also, if you try to access a different domain or server, you are asked for password information. The passwords and IDs are cached as long as the Cheyenne AntiVirus manager program remains open.

NOTE:For NDS-only users: the login ID you provide must be a distinguished (complete) name, for example: **`ADMIN.ACCOUNTING.WORK`**

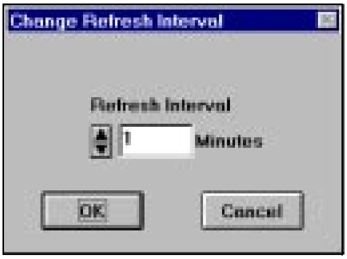
Using the NetWare Domain Manager

The Domain Manager can scan files on all domain member servers or on an individual member. The scanning can be scheduled or it can be run immediately. Scanning can be repeated at varying intervals. The actual scanning is done by Cheyenne AntiVirus's NLM on the server.

You can scan all of your domain members by setting up one scan job. The information for the scanning job is propagated to all of your domain members. For example, by setting up a job to scan the SYS volume on your master server, you scan the SYS volume on all of your domain member servers.

With the new Tree View Browser, you can have updated information of the various Cheyenne AntiVirus server readily available with automated update intervals and detail server information. You can even connect to a remote server with the new Point-to-Point Direct Connection functions.

The new Domain Manager also allows you to manually refresh the Tree View Browser, or configure it to automatically update the network tree information at a specific interval. To set the automatic refresh interval, you must select the *Domain* command at the menu bar, then the *Refresh* option, and the *Change Refresh Interval* command. This pulls up the Change Refresh Interval menu as such:


Change Refresh Interval

Refresh Interval: 1 Minutes

Instructions for a
an

Follow the instructions below to perform a basic scan of a domain using the Domain Manager.

1. Click the Domain button.

The Domain Manager screen appears:

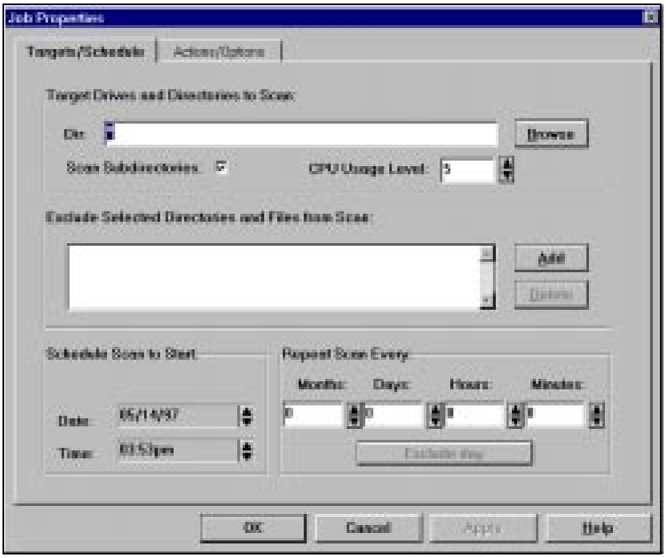
The symbols in the Domains/Servers window are explained below:

M	=	Master Server	The Master Server controls the members of its domain.
⊞	=	Expandable Domain	Double-click to see all of the member machines of this domain.
⊟	=	Expanded Domain	Click to collapse this domain.
	=	Single Server	This server is available to include in a domain.
	=	Orphan Domain	This domain was deleted. The master is now part of a new domain. This is not a normal condition. Delete the orphan domain and create a new domain.

2. Highlight a domain.

3. Click the Add/Re-Schedule a Scan Job button.

This button starts or schedules a job. The Job Properties window appears:



Dir: *

Scan Subdirectories ☑

CPU Usage Level: 5

Date: 05/14/97

Time: 03:52pm

Months: 0 Days: 0 Hours: 0 Minutes: 0

4. Enter information on the Schedule New Scan Job screen.

Target Drives and Directories to Scan

Enter the target drives, directories or volumes to scan. You can browse by clicking the Browse button.

NOTE:In the Dir: field, an asterisk (*) means Cheyenne AntiVirus will scan all of the volumes on the domain members. It will not scan floppy drives or mapped drives.

Scan Subdirectories

Check to scan all subdirectories beneath the scan source.

CPU Usage level

Enter a value from 1-99 percent. This allows you to adjust the maximum level of CPU utilization when running the Domain Manager. For example, if you set the field to 35 percent, Cheyenne AntiVirus scanning slows down if CPU utilization surpasses 35 percent.

Exclude Selected Directories and Files from Scan

You can exclude specific files or directories from being scanned. For example, you might want to exclude all files in a directory used for research purposes only.

To specify a file or directory, click Add. Type in the name of the file or directory and click OK. Since a file or directory may not exist on every machine, Cheyenne AntiVirus will only apply the exclusion to those machines that contain the file or directory you specified.

Schedule Scan to Start

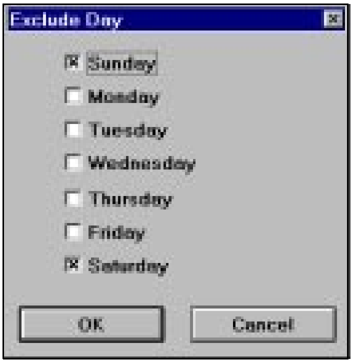
Indicate when the scan should run. The default is the current date and time.

Repeat Scan Every

If you want the scan to take place a single time, these fields should be left at zero.

If you want the scan to run at regular intervals, specify the time interval between each scan.

If you wish to exclude a particular day or days of the week from the scanning schedule, click the Exclude Day button. In the Exclude Day window, you can select one or more days on which a scheduled scan should *not* be run.



Exclude Day

☒ Sunday
□ Monday
□ Tuesday
□ Wednesday
□ Thursday
□ Friday
☒ Saturday

The Exclude Day button will only be active if at least one of the *Repeat Scan* fields is set to 1 or greater.

5. Click OK when done.

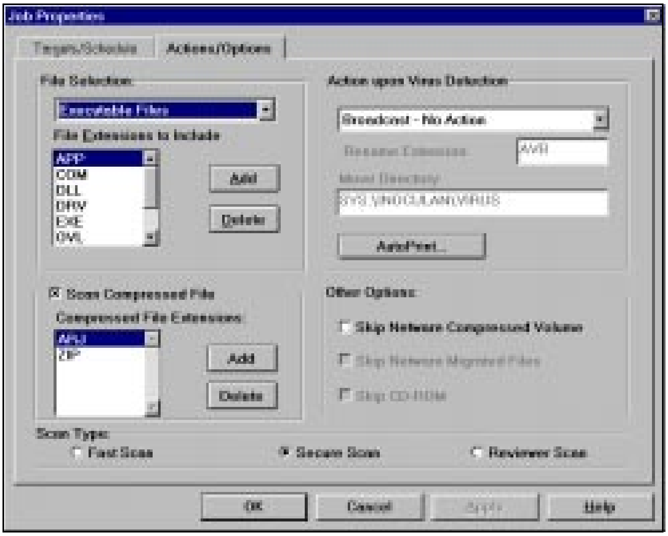
Actions and Options for Domain Scans

Cheyenne AntiVirus provides a host of actions and options to customize the scanning process, including selecting file types to scan, the action to take if a virus is found, and skipping or including certain kinds of files.

Cheyenne AntiVirus's scanning Actions

To apply an action:

1. Click the Actions/Options tab on the Job Properties screen.



Job Properties

File Selection: Executable Files

File Extensions to Include: APP, COM, DLL, DRV, EXE, OVL

☒ Scan Compressed File

Compressed File Extensions: ARJ, ZIP

Action upon Virus Detection: Broadcast - No Action

Rename Extension: AVB

Move Directory: SYS:\INOCULAN\VIRUS

Other Options:

□ Skip Netware Compressed Volume

□ Skip Netware Migrated Files

□ Skip CD-ROM

Scan Type: ○ Fast Scan ● Secure Scan ○ Reviewer Scan

2. Select the actions you want to include with the scanning job.

DOS File Selection

You can select all files or a selection of executable files. If you select *Executable Files*, you can further define which files to scan by their extensions.

Click the Add button to enter an executable file type.

To delete a file type from the list, highlight it and click Delete.

Action upon Virus Detection

Select one of the options described below. Regardless of which option you choose, a message is broadcast when a virus is detected.

NOTE: Cheyenne AntiVirus's Alert system can be configured to send a message to people in your organization when a virus is encountered. Messages can be sent via pager, e-Mail, FAX, NetWare broadcast, SNMP, or trouble-tickets sent to a printer. This assures that any viral infection on your network is immediately communicated to the people responsible for taking corrective actions. To configure the Alert service, refer to Chapter 6, "Alerting Users When a Virus is Detected."

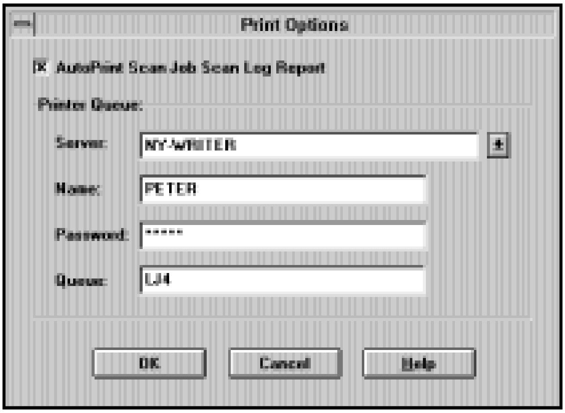
Action	Description
Report Only - No Action	Sends messages to Alert via Broadcast, MHS, Fax, SNMP, Trouble Ticket, and Pager, if they have been set up in Alert. The message also appears in the Scanning Report Log.
Delete File	Deletes an infected file from the machine.
Rename File	Renames infected files by giving them an *.AVB extension. Files with this extension will not be scanned by any of Cheyenne AntiVirus's scanners. If a file exists with the *.AVB extension and an infected file in the same directory will result in the same file name, the *.AVB extension will be changed. The extension will become *.AV# and the number will be incremented for each subsequent occurrence (*.AV0, *.AV1, etc.). For example, an infected MOUSE.COM is renamed MOUSE.AVB and then an infected MOUSE.SYS is renamed to MOUSE.AV0.
Cure File	Removes certain known viruses from infected files and restores the files to their original state. If the file cannot be cured, it will be renamed with an *.AVB extension (refer to 'Rename File' below). Even if Cheyenne AntiVirus cures the file, we recommend you purge the infected file and then restore the original file.

Action	Description
Move File	Moves an infected file from its current directory to the Cheyenne AntiVirus\VIRUS directory.
Purge File	Deletes an infected file so that it cannot be recovered (for example, using Novell’s Salvage utility).
Rename and Move File	Renames infected files by giving them a different extension and then moves them to the Cheyenne AntiVirus\VIRUS directory.
Copy and Cure File	Will make a copy of the infected file to the Cheyenne AntiVirus\VIRUS directory and continues to cure the file.

NOTE:If a virus is found in a compressed file, it will only be reported. Other scan actions - cure, rename, move, purge, delete - will not take place unless the file is decompressed. If at all possible, delete the file rather than decompress it.

AutoPrint

Select AutoPrint to automatically print the results of the job scan. When you click the AutoPrint button, the following screen appears:



Print Options

☒ AutoPrint Scan Job Scan Log Report

Printer Queue:

Server: NY-WRITER

Name: PETER

Password: *****

Queue: LJ4

Select a server using the drop-down list, then enter your user name and server password.

In the Queue field, enter your NetWare printer queue name. If you do not know your printer queue name, open the DOS prompt window, type PCONSOLE at the command line, and press Enter to access the NetWare Print Console. Select Print Queue Information from the menu to see your print queue choices. Press ESC to exit the Print Console and return to the DOS prompt.

For an NDS queue, you must provide a distinguished (complete) name.

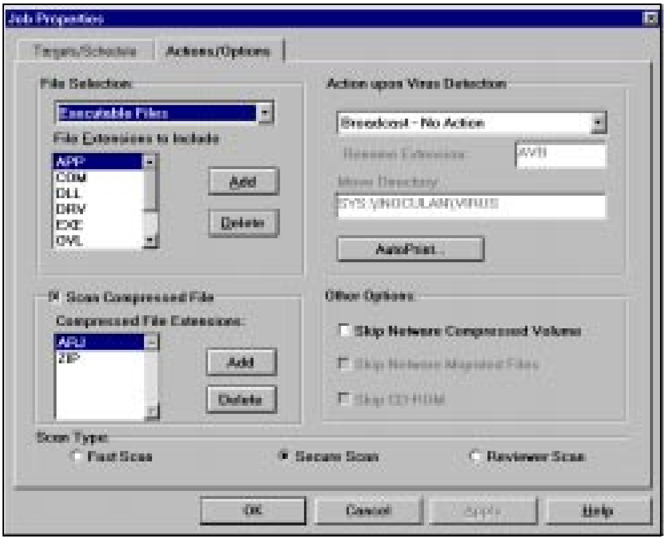
If you need additional instructions on how to use the Print Console, consult your NetWare administrator.

3. Click OK to set your Action selections, or click the Options tab to set scanning options.

Cheyenne AntiVirus's scanning Options

To set Cheyenne AntiVirus's scanning options:

1. Click the Actions/Options tab on the Job Properties screen.



File Selection: Executable Files

File Extensions to Include: APP, COM, DLL, DRV, EXE, OVL

Action upon Virus Detection: Broadcast - No Action

Rename Extension: AVB

Move Directory: SYS:\INOCULAN\VIRUS

☒ Scan Compressed File

Compressed File Extensions: ARJ, ZIP

Other Options:

□ Skip Netware Compressed Volume

□ Skip Netware Migrated Files

□ Skip CD-ROM

Scan Type: ○ Fast Scan ● Secure Scan ○ Reviewer Scan

2. Select the options you want to include with the scanning job.

Scan Type

Choose one of the following scanning options:

Scan Type	Description
Fast Scan	Checks just the beginning and end of each file. Using Fast Scan improves scanning efficiency when processing large groups of files. *However, it is possible for a file to have a virus that may be missed by Fast Scan*. Executable files (*.EXE, *.COM, etc.) are always fully scanned.
Secure Scan	Examines the entire file. This is a thorough way to check files but is slower than running a fast scan.
Reviewer Scan	Also examines the entire file. In addition, it searches for *virus-like* activity within files. Under unique circumstances, the Reviewer Scan may generate a false alarm. Therefore, use this scan only when the *Report Only - No Action* option is selected. You should use the Reviewer Scan to confirm the presence of a virus after a Fast or Secure scan has located a virus.

Skip Netware Compressed Volume

This option will cause Cheyenne AntiVirus to avoid scanning any NetWare compressed files on your servers. This is the default value. Scanning compressed files will increase the scanning time.

Skip Netware Migrated Files

The function is reserved for future use and is not available at this time.

Skip CD-ROM

This function is reserved for future use and is not available at this time.

Scan Compressed Files

Select this option for Cheyenne AntiVirus to scan compressed files. By default, Cheyenne AntiVirus scans files of the ZIP and ARJ format, as well as Microsoft compressed files. Microsoft compressed files end with an underscore, such as: STARTUP.EX_. (Note that if a Microsoft compressed file is contained *within* a ZIP file, it will not be scanned.) To add other file types, click the Add button.

3. Click OK when done.

Modifying a Scan Job

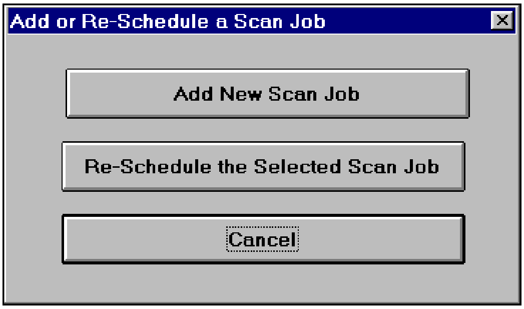
Once you have scheduled a new scan job, it can be modified to fit your requirements.

1. In the Domain Manager, click the Scan Job and Log View button.

   Highlight the scheduled job in the Job Queue Screen.

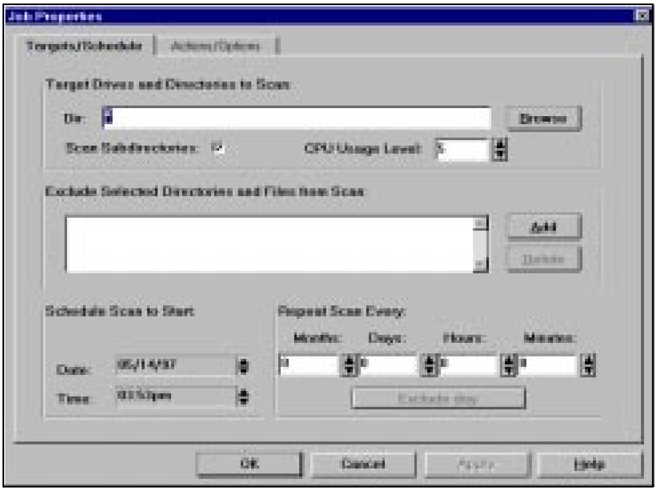
2. Click the Add/Re-Schedule a New Scan Job button, or double click on the specific scan job in the job queue.

3. The Add or Re-Schedule a Scan Job menu appears:


Add or Re-Schedule a Scan Job
Add New Scan Job
Re-Schedule the Selected Scan Job
Cancel

   Select an option.

4. The Job Properties screen is displayed once more:



Scan Subdirectories: ☑

CPU Usage Level: 5

Date: 05/14/97

Time: 03:53pm

Months: 0 Days: 0 Hours: 0 Minutes: 0

5. Make the changes in either the Job Properties screen, and the Actions/Options screen.

6. Click OK when done to resubmit the scan job.

Checking the Progress of Your Scan Job

You can view the steps of your scan while it is in progress.

1. In the Domain Manager, click the Scan Job and Log View button.

   The Scan Job Queue screen appears.

2. Double-click on the active job.

   The Job Scan Progress screen appears. Screen information is updated as the scan continues. The status bar at the bottom of the window shows what percentage of files have been scanned.

3. Click Close when done.

Checking the Results of Your Scan Job

Follow the instructions below to see the results of the Domain Scan:

1. Highlight a domain.
2. Click the Scan Job and Log View button.

   The screen displays the results of all Domain scanning jobs.
3. Double-click on a log in the Job Log Report window to view job details.

   This screen displays detailed information about the scanning job.

Scan Record settings

Cheyenne AntiVirus will keep from 10-2,000 records. When the file is full, the records will be purged in date sequence (oldest first). You can also set how long you wish to keep a record.

To set the Scan Record options:

1. Click the Configuration button in the Domain Manager window.
2. Click the Scan Record/Event Log tab.
3. Select the Scan Record options.

Maximum Messages

The maximum number of messages that should remain in the Scan Record. Values range from 10 to 2,000 lines.

Purge Records Time

Indicates how long, in days, you want to keep an event in the log. Values range from 1 to 365 days.

Message Filters

You can select the type(s) of message(s) that should be stored in the Scan Record.

Message Type	Description
Critical Message 🛑	This is the highest level message. It requires your immediate attention once logged. This message could mean, for example, that a virus was detected, or there is a critical problem on the network. This is the default and cannot be unchecked.
Warning Message !	The second priority message tells you if a scan was cancelled and no virus was found at that point.
Informational Message ℹ	This informs you of events that do not require a response, such as a scan has started or stopped, or a completed scan found no viruses.

4. Click OK when done.

NOTE:For more information on InocuLAN for NetWare management, consult the InocuLAN for NetWare Supervisor Guide.

Using the Local Scanner

The Local Scanner scans files on your local machine, on mapped drives, and on networked machines.

Local Scanner vs. domain management

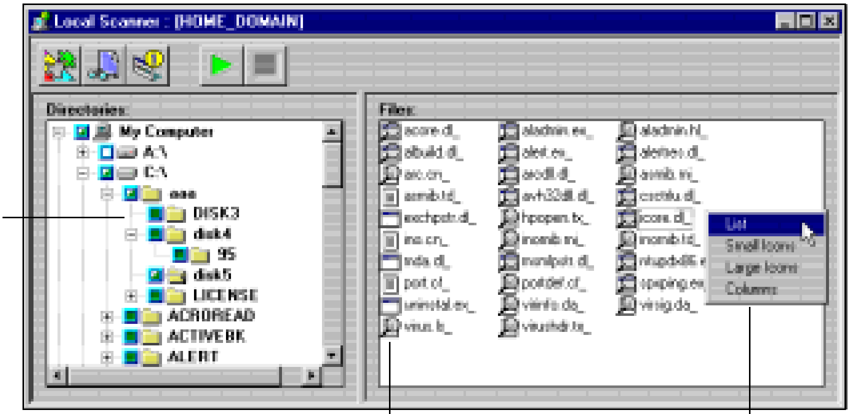
InocuLAN's domain management provides extensive protection for the NT enterprise. However, certain situations are more easily and effectively handled by the Local Scanner. For instance:

- Scanning a server that is not part of a network.
- Scanning a particular directory or file.
- Scanning a floppy diskette or CD.

How to use the Local Scanner

Follow the instructions below to use the Local Scanner.

1. Click the Local Scanner button to open the scanner:



The Explorer-style browser lets you select what to scan, right down to the individual file level.

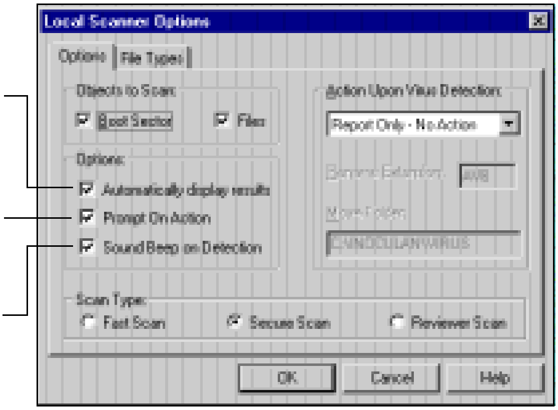
The magnifying glass icon indicates that a file will be scanned. Click a file to change the setting, or highlight a group of files and right-click to bring up the select/deselect button.

Right-clicking in the Files window lets you change the way files are viewed, using the same options found in the Windows Explorer.

2. Select the drives, directories and/or files you want to scan.

3. Set the scanning options by clicking on the Options button.

The Local Scanner Options dialog box will appear:



Local Scanner Options

Objects to Scan: ☑ Boot Sector ☑ Files

Options:
☑ Automatically display results
☑ Prompt On Action
☑ Sound Beep on Detection

Action Upon Virus Detection: Report Only - No Action

Rename Extension: AVB

Move Folder: C:\INOCULAN\VIRUS

Scan Type: ○ Fast Scan ● Secure Scan ○ Reviewer Scan

Click here to see scan results as soon as the scan is finished. Otherwise, you can view results in the Scan Log.

Click here to be notified before InocuLAN takes action on infected files.

Check here for InocuLAN to beep when a virus is detected.

4. Because we want to make all scans are as secure as possible, choose both Boot Sector and Files in the Objects to Scan field. If you suspected a floppy diskette had a boot sector virus, you might deselect Files to speed up the scanning process.

Scanning actions

5. You control what happens to an infected file in the Action Upon Virus Detection field.

   - Because you want to decide whether or not a file is cured on an individual basis, you choose the *Broadcast - No Action* option.
   - If you prefer that an infected file be deleted automatically, choose *Delete File.*
   - *Cure Files* removes viruses from infected files and restores the files to their original state. If the file cannot be cured, it is renamed with an AVB extension (refer to 'Rename File' below). Even if InocuLAN cures the file, we still recommend you to delete the infected file and then restore the original file from a backup or the product installation disks.
   - *Rename File* renames infected files by giving them an AVB extension. AVB files will not be scanned by InocuLAN. Infected files with the

same name will be given incremental extensions in the form AV#, for example: FILE.AV0, FILE.AV1, etc.

- *Move File* moves an infected file from its current directory to the INOCULAN\VIRUS directory.
- *Purge File* deletes an infected file so that it cannot be recovered.
- *Rename and Move File* renames infected files by giving them an AVB extension and then moving them to the INOCULAN\VIRUS directory.

Whenever an action is taken, InocuLAN sends messages via Broadcast, Microsoft Mail, Microsoft Exchange, SNMP, Trouble Ticket, and Pager, if they have been set up in Alert. The message also appears in the Scanning Log and the Windows NT Event Log.

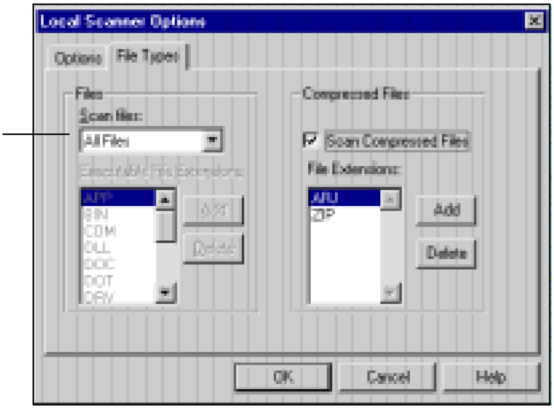
Scan Type

6. The level of scanning is set in the Scan Type field. Because you want to ensure that the files are scanned in their entirety, you choose Secure Scan. Fast Scan runs quicker than Secure Scan checking only the beginning and the end of each data file, the place where a virus is most likely to hide. Fast Scan improves scanning efficiency when processing large groups of data files, but it is possible for a file to have a virus that is missed by Fast Scan.

   If you suspect you have a virus but Secure Scan is not detecting one, you can use the *Reviewer Scan* option. The Reviewer Scan can also detect viruses that are inactive or have been deliberately modified, such as in a virus testing laboratory. Note that in unique circumstances, Reviewer Scan can generate a false alarm. Therefore, if you are using Reviewer Scan as your standard scanning option, you should use the Report Only option.

Selecting files to scan

7. Now that the scanning options are set, you have to select the types of files you want to scan. Click on the Files menu tab.



Scan files: All Files

☑ Scan Compressed Files

InocuLAN can scan all files, or you can include or exclude selected file types. You can also add and/or delete file types from the default list.

Scan Compressed file

8. Choose Scan Compressed File for InocuLAN to scan compressed files. By default, InocuLAN scans files of the ZIP and ARJ format, as well as Microsoft compressed files. These files end with an underscore, such as: START.EX_. To add other file types, click on the add button.

9. Click OK to accept the settings.

10. Click the Start/Continue Scanning Drive button. The scan begins immediately. Scanning job progress can be viewed in the Local Scanner window.

11. When the scan is completed, the Virus Scan Results window displays scanning information, including the name and location of any viruses that were found.

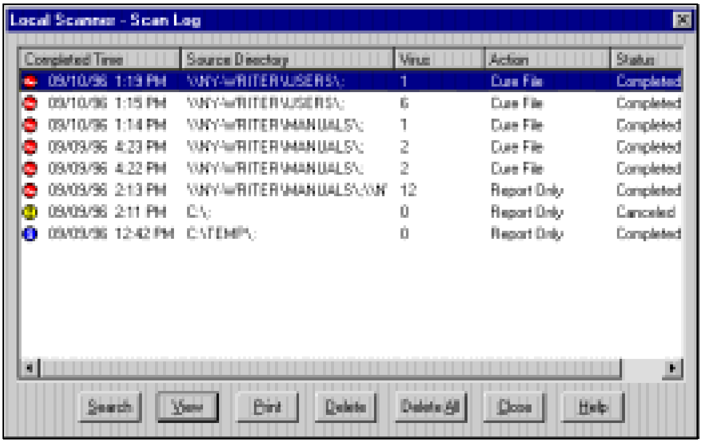
NOTE: The Local Scanner does not scan a mapped drive on a machine that is running InocuLAN's Real-time Monitor.

Checking the results of your scan

If you have the option *Automatically Display Results* selected, the results of your scan appears on the screen when the scan is completed.

If you do not have this option selected, or if you want to view the results at a later time, follow the instructions below:

1. Click the Scan Log button. The Local Scanner Scan Log appears:



Local Scanner - Scan Log

Completed Time	Source Directory	Virus	Action	Status
09/10/96 1:19 PM	\\NY-WRITER\USERS\:	1	Cure File	Completed
09/10/96 1:15 PM	\\NY-WRITER\USERS\:	6	Cure File	Completed
09/10/96 1:14 PM	\\NY-WRITER\MANUALS\:	1	Cure File	Completed
09/09/96 4:23 PM	\\NY-WRITER\MANUALS\:	2	Cure File	Completed
09/09/96 4:22 PM	\\NY-WRITER\MANUALS\:	2	Cure File	Completed
09/09/96 2:13 PM	\\NY-WRITER\MANUALS\:\\N	12	Report Only	Completed
09/09/96 2:11 PM	C:\:	0	Report Only	Canceled
09/09/96 12:42 PM	C:\TEMP\:	0	Report Only	Completed

2. Highlight the job you want to find out more information about.

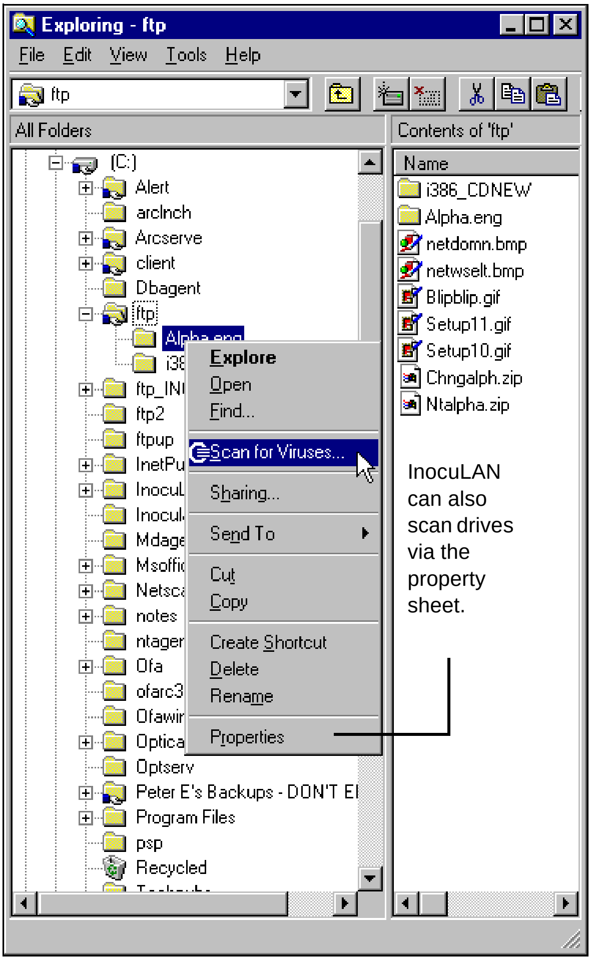
3. Click View or double-click on the job to view details of the scanning job.

Windows NT 4.0 Enhancement - Local Scanning shell extensions

If you are using Windows NT 4.0, you can quickly scan a directory or file by using InocuLAN's shell extensions.

To use the shell extensions, locate a directory or file in My Computer or the Windows Explorer. Right-click on the directory or file and select *Scan for Viruses...*, as shown at the left.

This will open the InocuLAN shell scanner. The shell scanner uses the same scanning engine and has the same functionality as the Local Scanner. To set the scanning options, click *Advanced*. (For information on scanning options, see section *How to use the Local Scanner*. Click Start to begin the scan. Scan progress will be shown by a moving progress bar. Scan reports are sent to the Local Scanner Scanning Log and can be reviewed there.



InocuLAN can also scan drives via the property sheet.

Internet-Enabled Download Protection

InocuLAN 4 for Windows NT protects NT servers from a rapidly-growing source of infections: Internet downloads.

Protection is automatic. If you selected Netscape Navigator and/or Microsoft Internet Explorer during the Internet Options portion of the InocuLAN installation, InocuLAN is already configured to work with your browser.

When you start a web page or FTP download with your browser, InocuLAN starts its Internet helper application to check the file for viruses while the download is taking place.

If no virus is detected, the Save box appears and you can proceed with your download. If a virus is detected, the file is moved to the Temp directory where it can be cured.

General suggestions

In addition to all of InocuLAN's features, we offer the following general suggestions to help keep your network virus-free:

- Set all of your executable files as *Read Only* files. Since a virus has the access rights of the user, making these files *Read Only* will reduce the chance of executable files becoming infected with viruses by non-administrator users.
- Be careful with administrator privileges. Logging in as an administrator or having administrator-equivalent privileges gives you access to the file server's directory structure. This means you can infect the entire directory structure if your workstation is infected with a virus. Therefore, you should not log in as a administrator unless you actually need administrator privileges to perform a task.
- Do not grant users *read* or *open* rights to other users' directories. Viruses can be spread if a user executes an infected program or copies an infected file from another directory.
- Use InocuLAN to scan floppy diskettes for viruses before copying any files from them.

- Back up your network after you successfully scan the network for viruses. This way, if InocuLAN detects a file with a virus that cannot be cured, you can restore a backed up, virus free version of that file.

3

Chapter

CONFIGURING SERVICES, LOGS AND BROADCASTS

InocuLAN's Service Manager lets you fine-tune your InocuLAN enterprise through configuration of Services, Logs and network Broadcasts.

In this chapter, you will learn:

Page

3-4 ➢ How to configure InocuLAN's services

3-6 ➢ How to configure the Event Log

3-8 ➢ How to configure the Scan Log

3-11 ➢ How to configure Broadcast Services

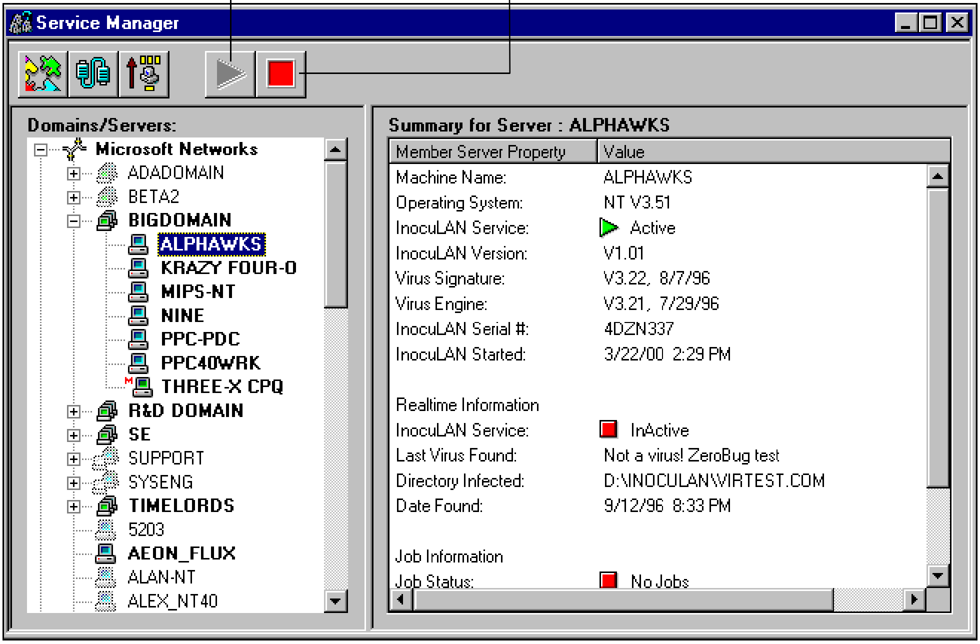
The Service Manager

InocuLAN's Service Manager allows you to start, stop and configure the InocuLAN service parameters.

Accessing the Service Manager

1. In the Quick Access Box, click the Service Manager button.

   The Service Manager Summary screen appears:



Click to start InocuLAN Services. By default, the services start when the server is started.

Click to stop InocuLAN services.

Service Manager

Domains/Servers:

- Microsoft Networks
  - ADADOMAIN
  - BETA2
  - BIGDOMAIN
    - ALPHAWKS
    - KRAZY FOUR-O
    - MIPS-NT
    - NINE
    - PPC-PDC
    - PPC40WRK
    - THREE-X CPQ
  - R&D DOMAIN
  - SE
  - SUPPORT
  - SYSENG
  - TIMELORDS
  - 5203
  - AEON_FLUX
  - ALAN-NT
  - ALEX_NT40

Summary for Server : ALPHAWKS

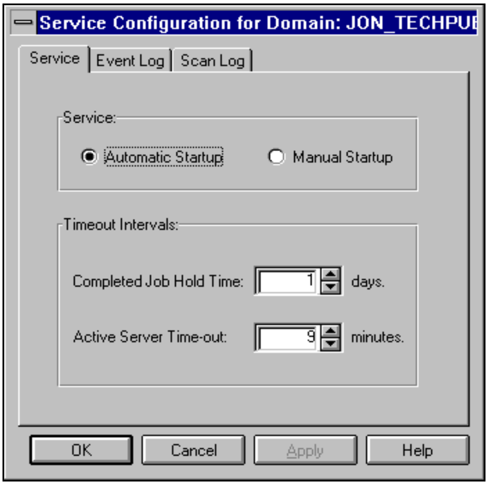
Member Server Property	Value
Machine Name:	ALPHAWKS
Operating System:	NT V3.51
InocuLAN Service:	▶ Active
InocuLAN Version:	V1.01
Virus Signature:	V3.22, 8/7/96
Virus Engine:	V3.21, 7/29/96
InocuLAN Serial #:	4DZN337
InocuLAN Started:	3/22/00 2:29 PM
Realtime Information	
InocuLAN Service:	🟥 InActive
Last Virus Found:	Not a virus! ZeroBug test
Directory Infected:	D:\INOCULAN\VIRTEST.COM
Date Found:	9/12/96 8:33 PM
Job Information	
Job Status:	🟥 No Jobs

Configuring InocuLAN's Services

This section explains how to configure InocuLAN services.

1. Click the Configuration button.

   The Service Configuration Screen appears:



Service Configuration for Domain: JON_TECHPUI

Service:

● Automatic Startup ○ Manual Startup

Timeout Intervals:

Completed Job Hold Time: 1 days.

Active Server Time-out: 9 minutes.

Automatic Startup

This option automatically starts the background services when the Windows NT machine is booted up.

Manual Startup

This option requires you to start up the InocuLAN Services manually via the Service Manager screen or the Windows NT Control Panel.

Completed Job Hold Time

Enter the number of days a finished job should remain in the Job Queue.

Active Server Time-out

Indicate how long InocuLAN should wait before considering a server inactive if the server has not sent any messages.

This feature works in conjunction with the Heartbeat Update Interval, explained on page 3-14.

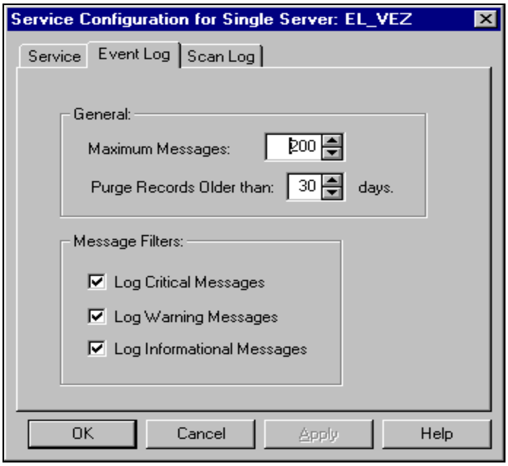
NOTE:The longer the time-out value, the longer it will take for the service to time-out an InocuLAN server. All InocuLAN machines should be configured with the identical value. If the values are different, some machines appear to be on-line while some appear to be off-line.

Configuring the Event Log

This section explains how to configure the InocuLAN Event Log.

1. In the Service Configuration screen, click the Event Log tab.

   The Event Log Configuration screen appears:



General:

Maximum Messages: 200

Purge Records Older than: 30 days.

Message Filters:

☑ Log Critical Messages

☑ Log Warning Messages

☑ Log Informational Messages

Maximum Messages — Indicate the maximum number of messages that should remain in the Event Log.

Purge Records Older than — Indicate how long you want to keep an event in the log.

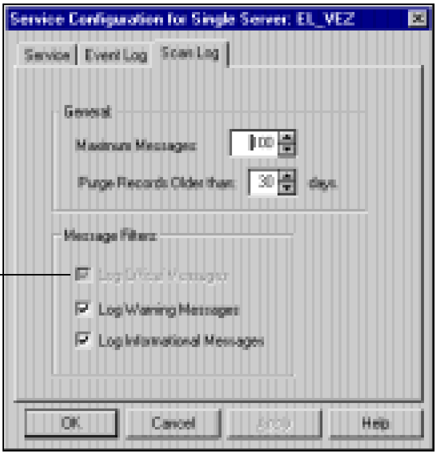
Message filters — You can select the type(s) of message(s) that should be stored in the Event Log.

- *Critical Message:* This is the highest level message. It requires your immediate attention once logged. This message could mean there is a virus detected, or there is a problem with the service. This is selected by default.
- *Warning Message:* The second priority message tells you if InocuLAN skips a file, and other non-critical information.
- *Informational Message:* This tells you if the service has started or stopped and if no viruses have been found.

Configuring the Scan Log

This section explains how to configure the InocuLAN Scan Log.

1. In the Service Configuration Screen, click the Scan Log tab. The Scan Log Configuration screen appears:



Maximum Messages: 100

Purge Records Older than: 30 days

☑ Log Critical Messages

☑ Log Warning Messages

☑ Log Informational Messages

This option cannot be deselected.

Maximum Messages

Indicate the maximum number of messages that should remain in the Scan Log.

Purge Records older than

Indicate how long you want to keep a scan record in the log.

Message Filters

You can select the type(s) of message(s) that should be stored in the Scan Log.

- Critical Message: A critical message alerts you when a virus is detected.
- *Warning Message:* A warning message tells you when a job was cancelled.

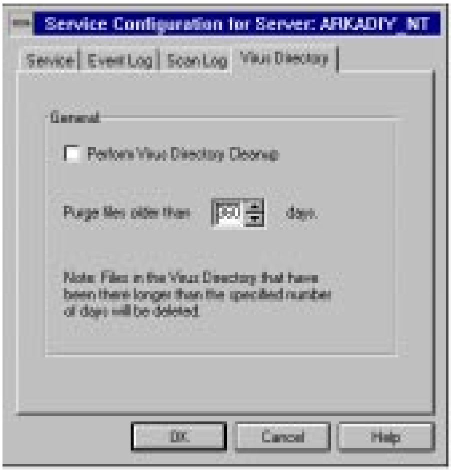
- *Informational Message:* An information message tells you when a job is completed with no viruses found.

Configuring the Virus Directory Purge

This section explains how to configure the InocuLAN Virus Directory Purge.

1. In the Service Configuration screen, click the Virus Directory tab.

   The Virus Directory Configuration screen appears:



Service Configuration for Server: ARKADIY_NT

General

□ Perform Virus Directory Cleanup

Purge files older than 360 days.

Note: Files in the Virus Directory that have been there longer than the specified number of days will be deleted.

Perform Virus Directory Cleanup

Check this box to schedule a full cleanup of the Virus Directory.

Purge files older than...

The number you enter represents the age of the files to be purged. For example, if you enter the number 360, any files that remain in the Virus Directory *longer* than 360 days are purged on Day 361.

Configuring Broadcast services

Applications often use a network broadcast to notify problems or errors to other workstations on the network.

InocuLAN may be configured to use the Mailslots protocol, TCP/IP protocol, or a combination of both. InocuLAN broadcasts include status changes, signature versions, engine versions, real-time and scheduled job status changes, and the OS version running on the server.

This section explains how to configure the InocuLAN broadcasts.

Hands-free configuration

InocuLAN 4 for Windows NT features a powerful network Auto Discover feature. InocuLAN machines can typically find each other on the network right out of the box, with no administrative intervention.

However, there are some instances when it may be necessary or desirable to manually alter some of the default settings. Possible scenarios that may require configuring include:

- Some of the InocuLAN machines cannot see each other. This may be due to routers blocking the InocuLAN broadcast signals, or sending messages to machines that are located on different IP subnets.
- You may wish to reduce broadcast traffic on your network. InocuLAN allows you to adjust the broadcast frequency to achieve the proper balance between accurate machine reporting and network throughput.

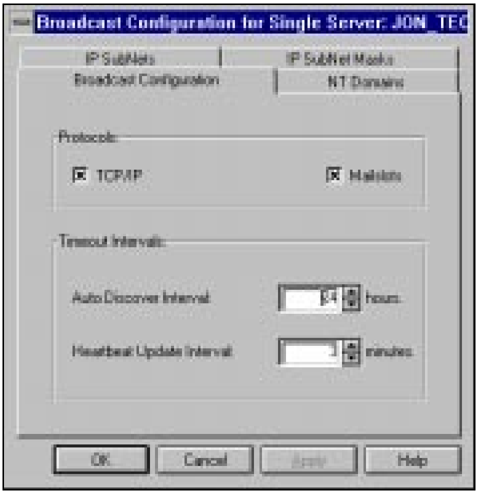
NOTE: Manual configuration of the InocuLAN network should be reserved for specific needs. It is recommend that the default values be tried initially. Because InocuLAN allows for very precise broadcast configuration, only an experienced network administrator should attempt to manually configure the software.

Configuring Broadcasts

InocuLAN's network broadcasts can be configured as shown below.

1. Click the InocuLAN Service Configuration button.

   The Broadcast Configuration screen appears:



Protocols

☒ TCP/IP ☒ Mailslots

Timeout Intervals

Auto Discover Interval 24 hours

Heartbeat Update Interval 1 minutes

Protocols

Mailslots and TCP/IP

Both settings are active by default. They allow InocuLAN to broadcast messages over both Mailslots (NT Domains) and TCP/IP (IP Networks) protocols. This setting is the most thorough. However, it may increase network traffic.

Mailslots configures InocuLAN to broadcast its messages over the Mailslots protocol only. Choose this if you have a mixed environment, and are certain that Mailslots broadcasts will reach all destinations.

TCP/IP configures InocuLAN to broadcast its messages over the IP protocol only. Choose this if you have an IP only network.

Time-out Intervals

Auto Discover Interval

Auto Discover allows InocuLAN to search your network for Windows NT domains and IP subnets. In a dynamic network, it is important that InocuLAN maintain a record of the machines it broadcasts to. InocuLAN maintains this record in three tables:

- NT Domain table - Auto Discover adds new NT Domains to this table (DOMAIN.TBL). This allows InocuLAN to broadcast via Mailslots to all machines in the listed Domain.
- IP Mask table - This table contains the local IP Mask (IPMASK.TBL) by default. If your environment supports more than one mask, they must be entered manually and the InocuLAN Service re-started.
- IP Subnet table - Once updated, InocuLAN uses the NT Domain and IP Mask tables to scan/add new IP Subnets to the IP Subnet table

(IPNET.TBL). This allows InocuLAN to broadcast via IP to all IP Subnets specified in the IP Subnet table.

Auto Discover adds NT domains and IP Subnets to these tables according to the hourly setting you choose.

NOTE:Please note that a zero (0) value disables Auto Discover.

Heartbeat Update Interval

This setting tells InocuLAN to broadcast a “Heartbeat,” or reminder broadcast, updating its status to the other InocuLAN machines on the network. This ensures that the status of all InocuLAN machines is known. The default time setting is three minutes.

NOTE:All InocuLAN machines should have the same Heartbeat Update Interval setting. Otherwise conflicting messages may be sent.

The Heartbeat Update Interval is set in conjunction with the *Active Server Time-out* setting, which is always three times (3x) the value of the *Heartbeat Update.* For example, if the Heartbeat Update Interval is set to five minutes, the Active Server Timeout will be set to 15 minutes, three heartbeats per timeout. You need only set one value: no matter which you set, the other automatically sets itself to the correct corresponding value.

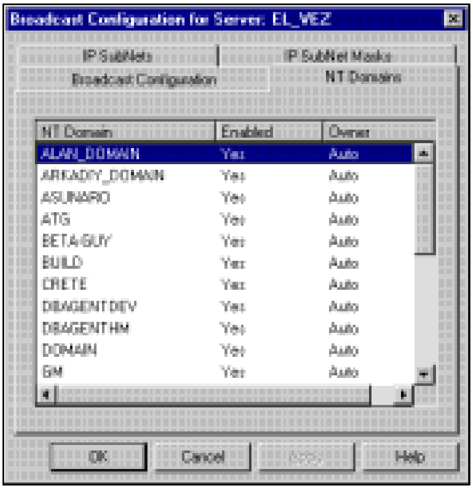
If a heartbeat is not received within the Active Server Timeout limit, the machine is considered down/inactive.

Configuring NT Domains

This section explains how to configure the NT Domains to which InocuLAN will be broadcasting. For InocuLAN to broadcast to an NT domain, the *Mailslots* protocol must be enabled.

To configure NT domains:

1. Select the NT Domains tab:



NT Domain	Enabled	Owner
ALAN_DOMAIN	Yes	Auto
ARKADIY_DOMAIN	Yes	Auto
ASUNARO	Yes	Auto
ATG	Yes	Auto
BETA-GUY	Yes	Auto
BUILD	Yes	Auto
CRETE	Yes	Auto
DBAGENT DEV	Yes	Auto
DBAGENT HM	Yes	Auto
DOMAIN	Yes	Auto
GM	Yes	Auto

All domains located by Auto Discover will appear in the list automatically.

Information entered here is added to the NT Domain table.

Adding/deleting domains

To add a new domain, press *Insert* and type the new name in the dialog box. To delete an existing domain, highlight it, and press *Delete*.

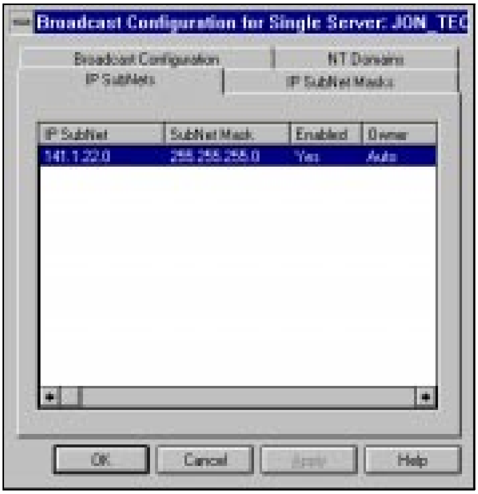
Changing the status of an existing domain

You can *enable*, *disable*, or *change the name* of the selected domain by double-clicking it and entering the proper information in the dialog box.

Configuring TCP/IP Networks

This section explains how to configure the IP Subnets to which InocuLAN IP broadcasts go.

For InocuLAN to broadcast to an IP Subnet, the *TCP/IP* protocol must be enabled.



Broadcast Configuration for Single Server: JON_TEC

IP SubNet	SubNet Mask	Enabled	Owner
141.1.22.0	255.255.255.0	Yes	Auto

Adding/deleting IP Networks

To add a new IP Network (IP Net and the IP Mask), simply press *Insert*, and type the new number(s) in the dialog box. To delete an existing IP Network, highlight it and press *Delete*.

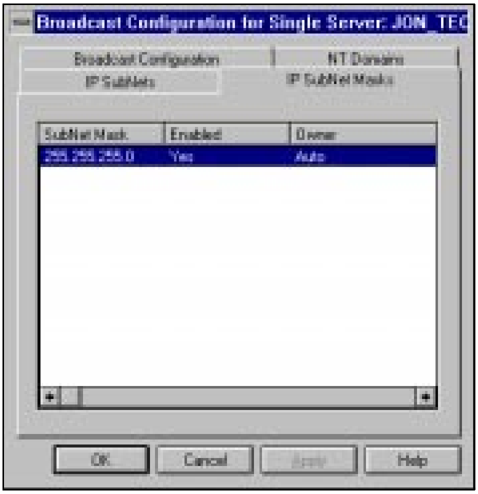
Changing the status of an existing IP Network

You can *enable*, *disable*, or *change the number(s)* of the selected IP Network by double-clicking it with the left mouse button and entering the proper information in the dialog box.

Configuring IP Network Masks

This section explains how to configure the IP Network Masks.

InocuLAN uses this information in the Auto Discovery of IP Subnets. (Refer to ‘Timeout Intervals’ on page 3-13 for more information on the Auto Discovery feature.)



SubNet Mask	Enabled	Owner
255.255.255.0	Yes	Auto

Information entered here is added to the IP Net table. The IP Net(s) entered supersedes the data found via the Auto Discovery feature.

Adding/deleting IP Network Masks

To add a new IP Network Mask, simply press *Insert*, and type the new number in the dialog box. To delete an existing IP Network Mask, highlight it, and press *Delete*.

Changing the status of an existing IP Network mask

You can *enable, disable,* or *change the number* of the selected IP Network Mask by double-clicking it with the left mouse button and entering the proper information in the dialog box.

Troubleshooting the InocuLAN network

If InocuLAN cannot see all of the InocuLAN machines in your environment:

1. Check the NT Domain table. It should contain all of the NT Domains. If a Windows NT Domain is not listed, manually add it to the NT Domain table.

2. Check the IP Subnet table. It should contain all of the IP Subnets. If an IP Subnet is not listed, manually add it to the IP Subnet table.

3. Check the Network Connections box of the Windows NT 3.51 File Manager or the Network Neighborhood of Windows NT 4.0. If these do not contain the InocuLAN machine(s) you are looking for, re-check your Windows NT configuration.

4. In a mixed InocuLAN domain of version 1.01 and 4, the Master Server must be an InocuLAN 4 machine.

5. Check that the Heartbeat Intervals are the same on all of your InocuLAN machines.

Synchronizing broadcast information

This feature allows an InocuLAN Administrator to update the Broadcast configuration of *all* InocuLAN machines on the network, based on the setting of one InocuLAN machine.

To synchronize InocuLAN broadcasts:

1. Open the Windows NT Registry Editor.

   In the Run dialog box, type the following command:

   REGEDT32.EXE.

2. Click OK.

   The Registry Editor screen appears. Follow the steps below:

Select HKEY_LOCAL_MACHINE

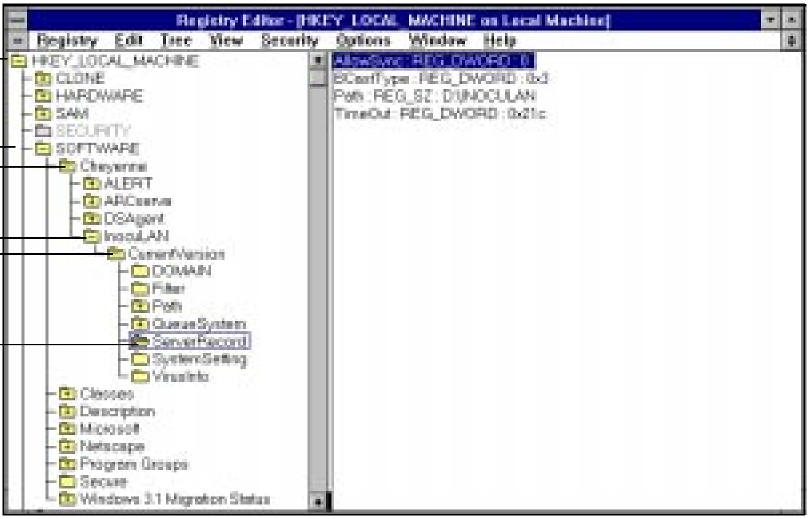
Scroll to *SOFTWARE*, and select it.

Next, select *Cheyenne.*

From within *Cheyenne*, click *InocuLAN*

Select *CurrentVersion.*

Scroll to *ServerRecord*, and select it.



```
AllowSync : REG_DWORD : 0
BCastType : REG_DWORD : 0x3
Path : REG_SZ : D:\INOCULAN
TimeOut : REG_DWORD : 0x21c
```

3. Once in the ServerRecord folder, highlight AllowSync: REG_DWORD.

   Note that the default value = 0

4. Click on AllowSync: REG_DWORD: 0. The DWord Editor dialog box will appear.

5. From within the DWord Editor, enter 1 in the Data column, and click OK.

   The AllowSync: REG_DWORD value will now read: 0x1.

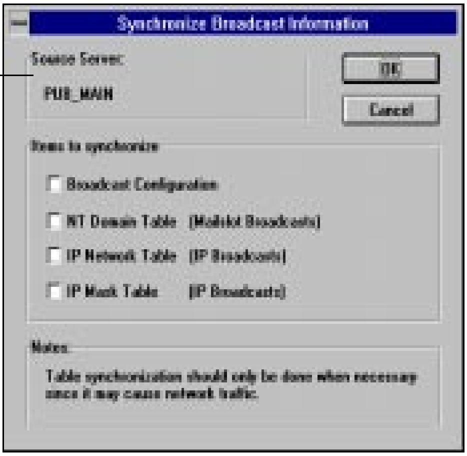
   This value activates the Synchronize feature.

6. Close the Registry Editor, and return to the InocuLAN Service Manager screen.

7. From the InocuLAN Service Manager Menu, highlight Service and select Synchronize.

   The Synchronize Broadcast information dialog box will appear:

The Source Server from which InocuLAN will be synchronizing all of the network InocuLAN computers.



Source Server:

PUB_MAIN

Items to synchronize

□ Broadcast Configuration

□ NT Domain Table [Mailslot Broadcasts]

□ IP Network Table [IP Broadcasts]

□ IP Mask Table [IP Broadcasts]

Notes:

Table synchronization should only be done when necessary since it may cause network traffic.

Select the items you wish to synchronize.

NOTE:Please make sure that you are using the correct Source Server. The broadcast settings for all other InocuLAN computers will be based on this server!

8. Select the items you wish to synchronize.

9. Click OK.

   Synchronizing the servers may take a few minutes to complete.

4

Chapter

AUTOMATIC DOWNLOAD, DISTRIBUTION AND UPDATE

InocuLAN's hands-free AutoDownload and distribution functions keep your network up-to-date with minimal user effort.

In this chapter, you will learn:

Page	
4-2 ➢	How AutoDownload and distribution work
4-5 ➢	How to use the AutoDownload Manager
4-12 ➢	How to configure Software Distribution

Automatic Signature Download, Distribution and Update

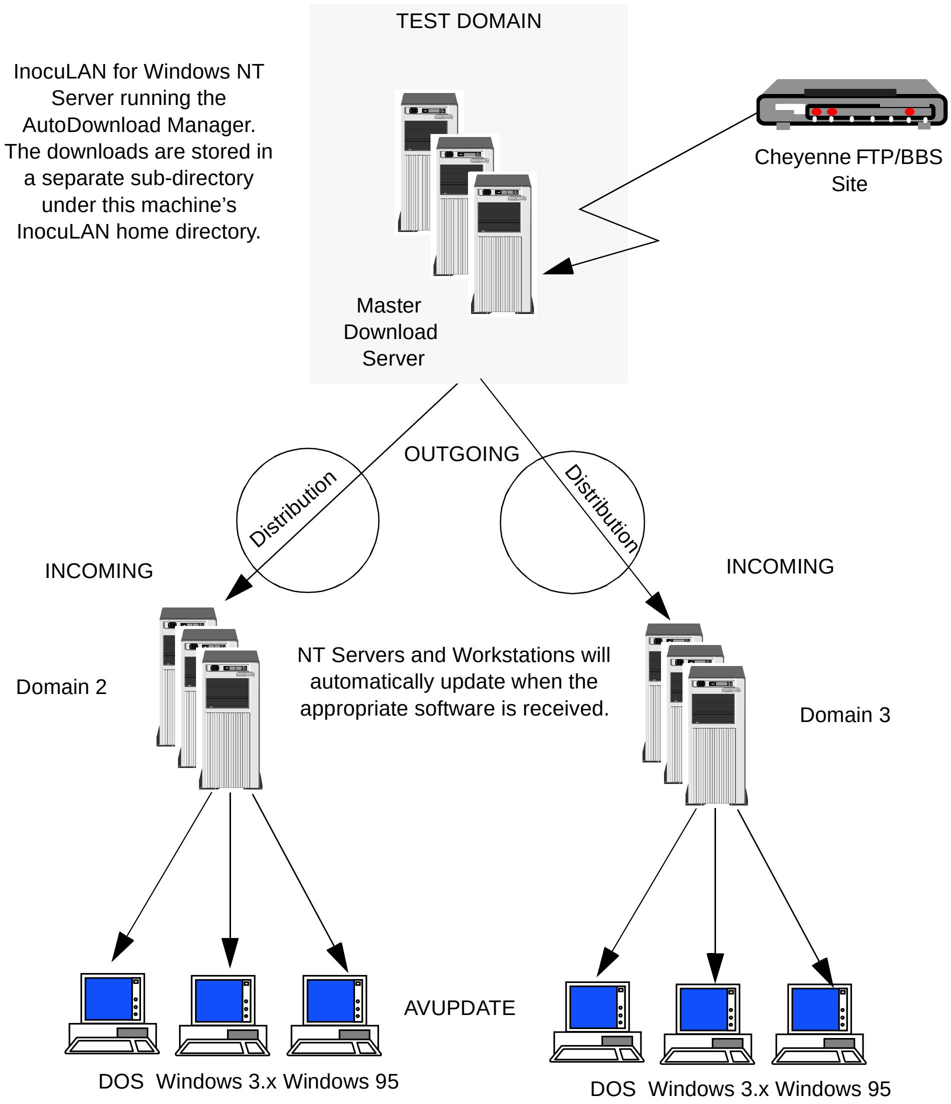
One of the most significant features of InocuLAN 4 for Windows NT is the ability to automatically download and distribute the latest signature files and software updates. InocuLAN includes a utility called AutoDownload which retrieves the latest files from the Cheyenne InocuLAN update site, either via FTP or via modem, and stores them in an InocuLAN sub-directory. InocuLAN then distributes these files to other InocuLAN servers. The AVUPDATE program can also be used to update files on Windows 95, Windows 3.x and DOS workstations when they log in to servers running InocuLAN.

NOTE:To prevent you from overwriting the pre-configured AVUPDATE.INI files, when you download or install InocuLAN on your server(s), the AVUPDATE file is initially named AVUPDATE.INO. You can rename this file later.

The following outlines the sequence of events needed to update an InocuLAN network:

- AutoDownload retrieves the signature files and software updates and stores them in the AutoDownload directory (called GBBSdata).
- InocuLAN's Distribution function on the AutoDownload machine then copies the files from the GBBSdata directory into the InocuLAN distribution directory (called Update), where they will be made available to other InocuLAN machines. Distribution parameters are provided to specify when to retrieve files, what platforms and languages to retrieve, and what server(s) to get them from.

- Other InocuLAN machines access the Update directory for files and update themselves based on pre-set parameters.
- Windows 95, Windows 3.x and DOS clients are updated when they log in to a Windows NT domain set up to run the AVUPDATE program from a login script. (Please see the Release Notes for details about AVUPDATE.)



InocuLAN for Windows NT Server running the AutoDownload Manager. The downloads are stored in a separate sub-directory under this machine's InocuLAN home directory.

NT Servers and Workstations will automatically update when the appropriate software is received.

InocuLAN Client Workstations.

InocuLAN for Windows NT AutoDownload and File Distribution system.

AutoDownload, Distribution and Update: A Scenario

AutoDownload and distribution is a very powerful feature of InocuLAN 4 for Windows NT. Once set up, the system automatically downloads files, distributes them across the network, and updates all InocuLAN machines, each step carefully controlled by InocuLAN's extensive feature set.

To best explain the concept and procedures of AutoDownload and distribution, the following pages outline a sample distribution scenario.

The network in our scenario consists of the following:

- A test InocuLAN domain called R&D DOMAIN. This domain consists of a Master Server and three member servers.
- A full production network of InocuLAN machines.

Our AutoDownload and distribution plan has four distinct stages:

- Stage 1: To download the latest InocuLAN files from Cheyenne Software. Files will be downloaded by the Master Server on R&D DOMAIN.
- Stage 2: The Master Server will access the new files and update itself based on pre-set parameters. The Master Server holds the files for three days before making them available to the other machines in R&D DOMAIN.
- Stage 3: At the end of three days, the new files on the Master Server becomes available to the member machines in R&D DOMAIN. Those machines, in turn, automatically update and run

with the new software. The member machines make the software available to the production machines after four more days pass.

- Stage 4: After a total of seven days, the files are made available to our production machines, which retrieve them and automatically update their software.

Stage 1 - Downloading the files

The first step is to retrieve the latest InocuLAN virus signatures and software updates. The AutoDownload Manager program handles the acquisition of virus signatures and software updates from the Cheyenne site by using FTP or modem connections.

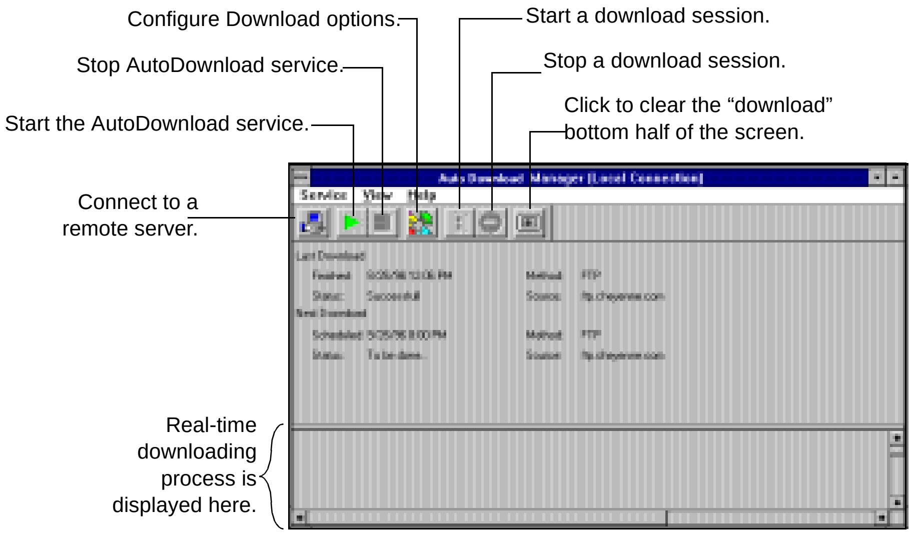
The AutoDownload Manager allows the user to change the default download date and time. InocuLAN is shipped with a monthly update setting.

NOTE:When first installing InocuLAN 4, it is recommended that you run a manual file download to ensure that the most current files are available. The AutoDownload service should be configured to start automatically on the machine you are using for downloading. This can be done using the Control Panel.

Begin by configuring the Master Server on R&D DOMAIN to download the new files:

1. Start the AutoDownload Manager icon from the Program Manager in Windows NT 3.51 or from the Start menu under Programs, InocuLAN for Windows NT in Windows NT 4.0.

The AutoDownload main screen appears showing the last and next download to take place:



Configure Download options.

Stop AutoDownload service.

Start the AutoDownload service.

Connect to a remote server.

Start a download session.

Stop a download session.

Click to clear the “download” bottom half of the screen.

Real-time downloading process is displayed here.

Last Download

Finished: 9/25/96 12:06 PM Method: FTP

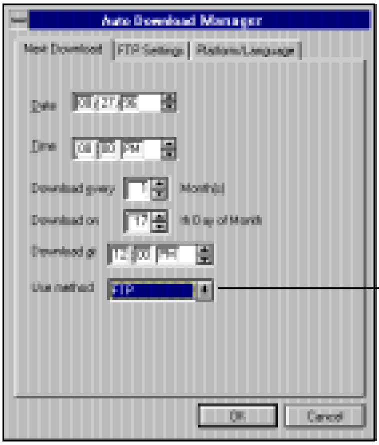
Status: Successful Source: ftp.cheyenne.com

Next Download

Scheduled: 9/25/96 8:00 PM Method: FTP

Status: To be done... Source: ftp.cheyenne.com

2. Next, click on the Download option toolbar button.



Date 08/27/96

Time 08:00 PM

Download every 1 Month(s)

Download on 17 th Day of Month

Download at 12:00 PM

Use method FTP

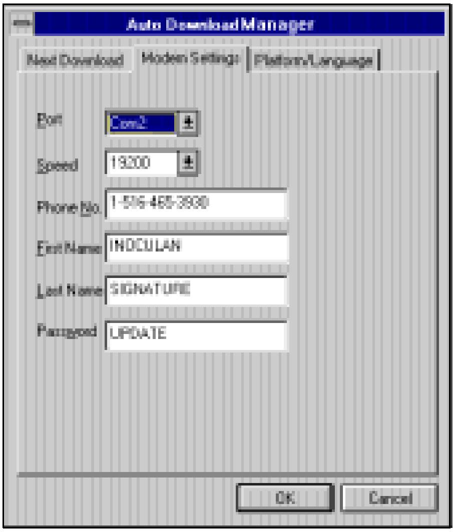
Click on the combo-box and select either *Modem (BBS)* or FTP to connect to the Cheyenne site.

NOTE:The minimum scheduled download period is one month.

The *Next Download* tab allows you to schedule the time, date, and month of the download.

3. Two methods of downloading are available.
   - Use FTP to connect to the Cheyenne site. The FTP site address is ftp.cheyenne.com. Enter the email address in the *Email Address* field.

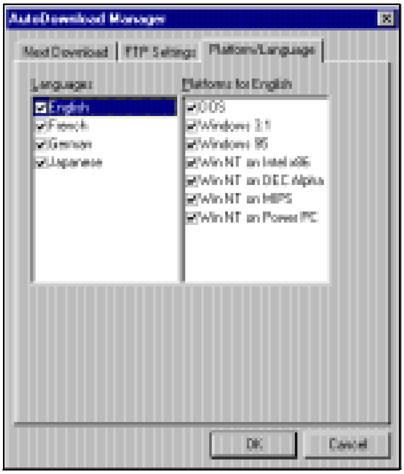
- You can also connect using a dialup asynchronous modem. If you highlight “Modem (BBS)” from the *Use method* sub-menu, the FTP Settings tab changes to *Modem Settings*.



Port: Com2
Speed: 19200
Phone No.: 1-516-465-3930
First Name: INOCULAN
Last Name: SIGNATURE
Password: UPDATE

The modem information is entered in the appropriate fields. The *First Name*, *Last Name*, and *Password* fields default to the correct information.

4. Next click on the Platform/Language tab.



Languages:
☑ English
☑ French
☑ German
☑ Japanese

Platforms for English
☑ DOS
☑ Windows 3.1
☑ Windows 95
☑ Win NT on Intel x86
☑ Win NT on DEC Alpha
☑ Win NT on MIPS
☑ Win NT on Power PC

Because you have a large network that has multiple platforms and languages, select and download all the available files.

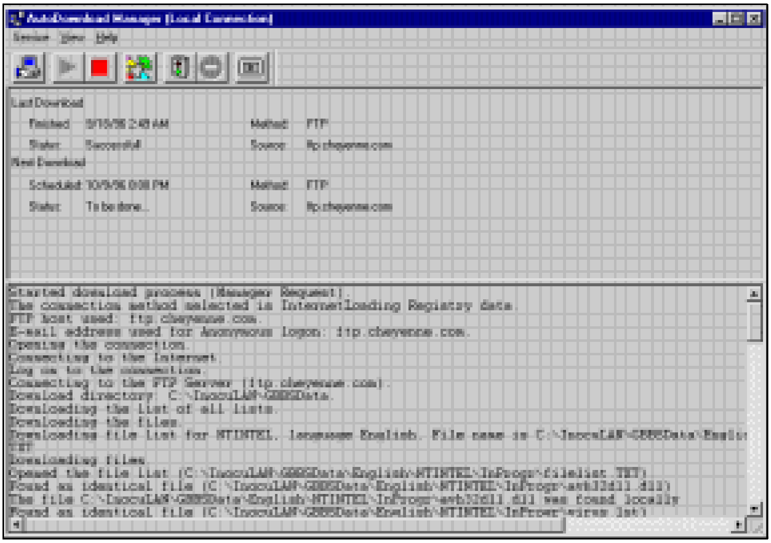
5. Click OK when completed.

6. Before the download takes place, start the service by clicking the Start AutoDownload service toolbar button.

When the service is started, the “traffic light” toolbar button becomes active. Click this button to run the download session immediately, rather than waiting for a scheduled time.

NOTE: The AutoDownload *Service* should not be mistaken for the AutoDownload download *session*. The service, like other Windows NT services, must be started before any actual client/server activity can occur.

When the downloading has completed, a screen similar to the one below is displayed:



Last Download

Finished 9/15/96 2:49 AM Method: FTP

Status: Successful Source: ftp.cheyenne.com

Next Download

Scheduled: 10/9/96 0:08 PM Method: FTP

Status: To be done... Source: ftp.cheyenne.com

```
Started download process (Manager Request).
The connection method selected is InternetLoading Registry data.
FTP host used: ftp.cheyenne.com.
E-mail address used for Anonymous logon: ftp.cheyenne.com.
Opening the connection.
Connecting to the Internet.
Log on to the connection.
Connecting to the FTP Server (ftp.cheyenne.com).
Download directory: C:\InocuLAN\GBBSData.
Downloading the list of all lists.
Downloading the files.
Downloading file list for NTINTEL, language English. File name is C:\InocuLAN\GBBSData\Englis
TXT
Downloading files.
Opened the file list (C:\InocuLAN\GBBSData\English\NTINTEL\InProgr\filelist.TXT)
Found an identical file (C:\InocuLAN\GBBSData\English\NTINTEL\InProgr\arb32dll.dll)
The file C:\InocuLAN\GBBSData\English\NTINTEL\InProgr\arb32dll.dll was found locally
Found an identical file (C:\InocuLAN\GBBSData\English\NTINTEL\InProgr\virus.lst)
```

The downloaded files are stored in the GBBSdata sub-directory. *Note that AutoDownload only retrieves the files from Cheyenne Software.* It does not distribute them. File distribution is a separate process (see next section for details).

7. The download session is complete, and we exit AutoDownload.

NOTE: The AutoDownload service is still running. Only the download "interface" or manager has been closed. You can always start up the AutoDownload manager to view the upcoming download schedule or configurations without having to restart the AutoDownload service. It is recommended that the AutoDownload service be configured for automatic startup on all machines that is used for downloads. This value is set through the Control Panel.

Summary of Stage 1:

As Stage 2 begins, we have completed AutoDownload and retrieved updates for all languages and platforms. These files are residing in the GBBSdata sub-directory of InocuLAN on the R&D DOMAIN master server. *At this time, the files have not yet entered the InocuLAN system.* The AutoDownload process only retrieves the files, it does not distribute them.

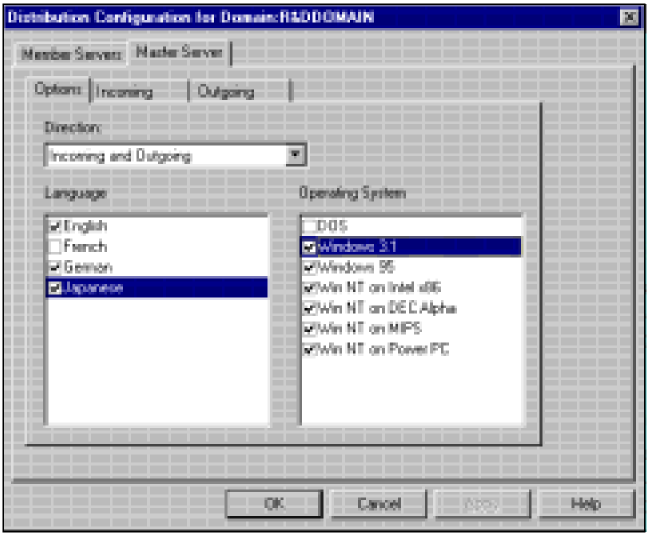
The next step is to update the Master Server of R&D DOMAIN.

Stage 2 - Updating the Master Server

To begin the process:

1. Start up the Service Manager from the Quick Start menu.

2. Click on the Configure Distribution Subsystem button. The options screen appears:



Distribution Configuration for Domain:R&DDOMAIN

Direction: Incoming and Outgoing

Language:
- ☑ English
- □ French
- ☑ German
- ☑ Japanese

Operating System:
- □ DOS
- ☑ Windows 3.1
- ☑ Windows 95
- ☑ Win NT on Intel x86
- ☑ Win NT on DEC Alpha
- ☑ Win NT on MIPS
- ☑ Win NT on Power PC

3. You are configuring the Master Server in R&D DOMAIN, so select the Master Server tab.

4. Because you want to control both the incoming and outgoing settings, select Incoming and Outgoing in the Direction field.

Distribution Tips

It is very important to understand the meaning of Incoming and Outgoing in the software distribution system.

Incoming parameters determine from where to get files, when to get them, and how often to check for them. These files can be retrieved from the local AutoDownload directory (GBBSdata) or from another InocuLAN machine.

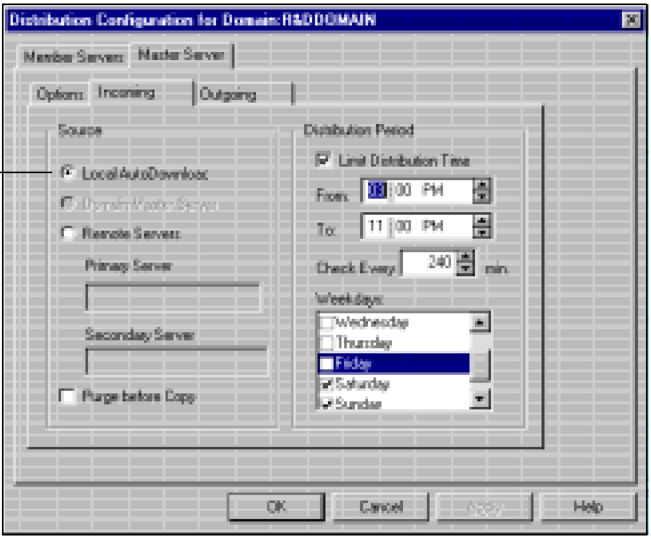
Outgoing refers to the files that a given server makes available to other InocuLAN machines.

5. While the enterprise uses all of the listed languages, the French network is currently undergoing repair. Therefore, you are temporarily not updating those machines, deselect French in the Languages field. (Note that you did download the French updates because we want to have them available. They will remain in the GBBSdata directory.)

6. Because no one in the enterprise is using DOS-based machines, deselect DOS in the Operating Systems field.

7. The next step is to determine from where (the Source) and when (the Distribution Period) the files enter the InocuLAN system. Click on the Incoming tab.

This will retrieve files from the local GBBSdata directory.



Source

● Local AutoDownload

○ Domain Master Server

○ Remote Servers

Primary Server

Secondary Server

□ Purge before Copy

Distribution Period

☑ Limit Distribution Time

From: 08 :00 PM

To: 11 :00 PM

Check Every 240 min.

Weekdays:

□ Wednesday

□ Thursday

□ Friday

☑ Saturday

☑ Sunday

8. Since you downloaded the files to the InocuLAN Master Server and now want to bring those files into the InocuLAN system, select Local AutoDownload: i.e., use the files on this machine’s hard drive, stored in GBBSdata.

9. If you had used the Distribution function before, there might already be files that were moved into the InocuLAN system. You can eliminate those files by choosing the Purge Before Copy function. If you do not select this option, identically named files are overwritten, and other files remain.

10. Because you don’t want the Master Server getting files during the week, restrict the distribution/update to the weekend.

To do so, select *Limit Distribution Time,* and under Weekdays choose *Saturday* and *Sunday.* However, your full system backups take place early on Saturday morning. Therefore, further limit the distribution time by choosing *From 3:00 PM to 11:00 PM.* This leaves ample time for your backups in the morning, and for file distribution in the afternoon.

Summary of Stage 2:

With these settings, the Master Server retrieves the new software updates after 3:00 PM on Saturday from the local GBBSdata directory. (The GBBSdata directory is only accessed locally.) Upon retrieving the files, the Master Server begins the update process. (*Only* the Master Server is updating at this time.) During the update, the InocuLAN service is temporarily stopped to allow files to be copied. Upon completion, the service restarts automatically.

In the next step, configure the outgoing parameters so that the Master Server runs with the new software for three days before other machines are given access.

Stage 3 - Updating the R&D DOMAIN member machines

1. Before other machines can retrieve files from the Master Server, the Outgoing parameters must be set. Click on the Master Server Outgoing tab:

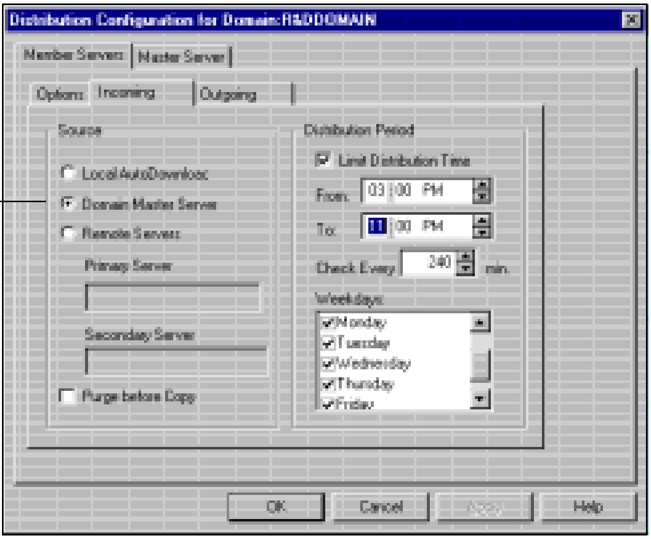
   Outgoing determines when other machines in our InocuLAN network can get new files from the machine we are configuring.

   To prevent the member machines (Member1, Member2 and Member3) from accessing the software too soon, set *Outgoing delay* on the Master Server to three days. Doing so holds the files on the Master Server for three days before they are distributed to rest of R&D DOMAIN. Remember that the three day delay does not apply to the Master Server, which is already updated with new software.

2. Click on OK when completed.

3. The next step is to configure the member machines to retrieve software from the Master Server.

   Click on the *Member Servers* tab, and select *Incoming*.



Files will be retrieved from the Domain Master Server.

Distribution Configuration for Domain:R&DDOMAIN

Source

○ Local AutoDownload
● Domain Master Server
○ Remote Servers
Primary Server:
Secondary Server:
□ Purge before Copy

Distribution Period

☑ Limit Distribution Time
From: 03:00 PM
To: 11:00 PM
Check Every 240 min.
Weekdays:
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday

4. Since the domain member machines retrieves their update files from the domain Master Server, we click the Domain Master Server button as the Source.

   As we recall, the Master Server received its files on Saturday and holds them for three days: that is, they will be made available on Tuesday.

5. Because you plan to update our production network four days from now using the files on the R&D DOMAIN member machines, click the Outgoing tab for the Member Servers and set the Outgoing Delay to four days.

Summary of Stage 3:

The member servers in R&D DOMAIN are now configured to take the new software from the Master Server.   After the Master Server's three day Outgoing Delay passes, the member machines access the software, copy it, and begin the updating process. The member machines, as the Master Server did, shut down briefly while the updates take place, and automatically restart afterwards.

The member machines run the new software for four days, at which time it is made available to the production network.

So far, Stage 2 and Stage 3 have allowed us seven days of running the software in our test environment. Schedule a seven-day cycle in order for the production machines to update on Saturday, one week after the process began, when they are not heavily used.

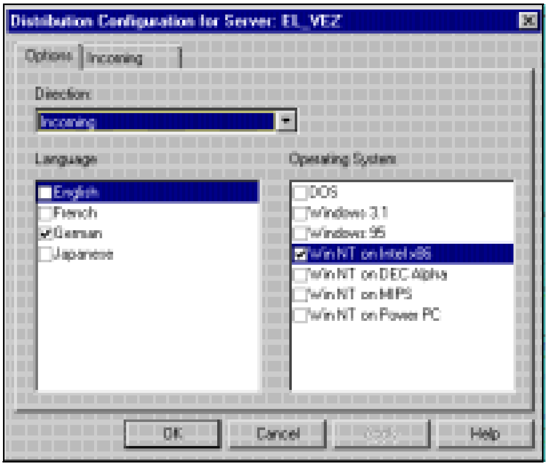
Stage 4 - Updating the Production network

The final stage is to move the new software into the production network.

All of your InocuLAN machines and InocuLAN domains are configured to retrieve software from the R&D DOMAIN machines. A great deal of variation is possible at this point.

The steps below illustrate some of the possibilities.

1. The first production machine configured is named El_Vez. Because El_Vez is a German language, Intel-based Windows NT machine, you need only retrieve that configuration. On the Options tab of El_Vez, we select German and Win NT on Intel x86.



Distribution Configuration for Server: EL_VEZ

Direction: Incoming

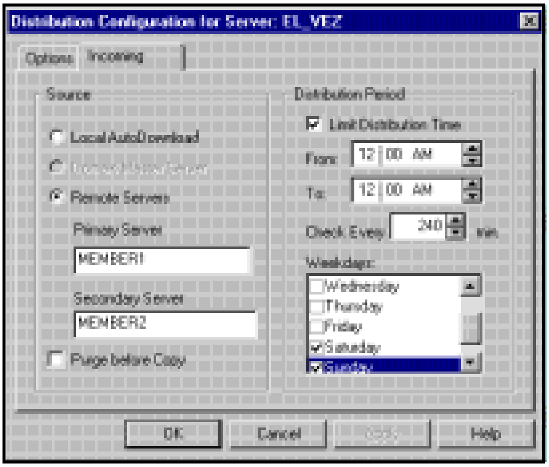
Language

□ English
□ French
☑ German
□ Japanese

Operating System

□ DOS
□ Windows 3.1
□ Windows 95
☑ Win NT on Intel x86
□ Win NT on DEC Alpha
□ Win NT on MIPS
□ Win NT on Power PC

2. We decide that El_Vez should retrieve its files from machine MEMBER1 of R&D DOMAIN. In the Primary Server field, we enter MEMBER1. As a precaution, we enter MEMBER2 in the Secondary Server field.



Distribution Configuration for Server: EL_VEZ

Source

○ Local AutoDownload

● Remote Servers

Primary Server: MEMBER1

Secondary Server: MEMBER2

□ Purge before Copy

Distribution Period

☑ Limit Distribution Time

From: 12:00 AM

To: 12:00 AM

Check Every: 240 min.

Weekdays:

□ Wednesday
□ Thursday
□ Friday
☑ Saturday
☑ Sunday

3. Because El_Vez is a production machine that should only update on weekends, click Limit Distribution Time and the Saturday and Sunday buttons under Weekdays.

   Leave the time at the default settings because you are not concerned about what time on the weekend the update will occur.

4. Since no other machines are retrieving files from El_Vez, we do not set any Outgoing parameters.

   Click OK to set the parameters.

5. Continue to similarly configure all the InocuLAN machines in your enterprise, each one set to retrieve precisely the version of the software that it requires.

<u>Summary of Stage 4:</u>

When all our production machines are configured, the entire enterprise has been automated.

In sum, each month the following will occur:

- The R&D DOMAIN Master Server automatically contacts the Cheyenne Software FTP site and download the latest InocuLAN updates.
- The Master Server updates itself on the first Saturday following the download. It runs the software for three days.
- On the following Tuesday, the member machines in R&D DOMAIN updates with software retrieved from the Master Server. They will run an additional four days.
- One week after the process began, all machines in our InocuLAN production network retrieves the correct software and update automatically.

Thus configured, the InocuLAN network requires no user intervention to always have the most current virus signature files and software updates running on all machines.

Updating of Client Workstations

The AVUPDATE program allows you to automatically install Cheyenne AntiVirus on Windows 95 and Windows 3.x/DOS workstations as users log in to a Windows NT server.

NOTE:If you are using AVUPDATE only for updating workstation software, please read “Updating Workstation Software” on page 4-26.

Understanding the process

To better understand AVUPDATE, a brief overview of the process is useful.

Installation files for Cheyenne AntiVirus are kept on a Windows NT server. Modifications are made to the server login script to run AVUPDATE. The script is assigned to all user accounts that need to have AntiVirus installed.

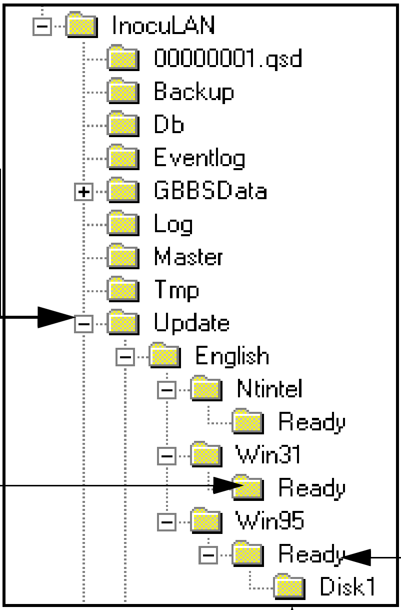
When a user logs in to the NT server, the login script runs the AVUPDATE program, which copy the appropriate files (Win 95 or 3.x/DOS) to the workstation and installs them. The entire process takes place with no intervention on the user’s part, allowing for fully centralized administration. (A workstation re-boot is needed to activate the AntiVirus real-time scanning. Users receive a message informing them of this.)

To set up automatic software installation:

Put the software on the server

1. The AntiVirus installation files must be properly placed on the server. These files are copied from the AntiVirus CD into the following directories which must be created under the InocuLAN/Update directory:

2. If you have previously used the InocuLAN AutoDownload and Distribution feature, some of the above directories may already exist.



The Update directory is shared as **cheyupd$** when the InocuLAN service is running. When the service is stopped, the directory is no longer shared.

Run the Setup program and install the program files on the NT server, or install them on a workstation, then copy the files to the following directory: Update\English\Win31\Ready

If you have an AntiVirus CD, copy the Windows 95 installation files to the following directory: Update\English\Win95\Ready

If you have AntiVirus on floppy diskettes, create the “Disk1” directory and copy the software to it. If you are installing AnitVirus from a diskettes, you will also need to create a “Disk2” directory.

Update the login script

This line tells WIndows NT machines not to run the AVUPDATE program.

3. Modify the login script used on the NT server by adding the following exactly as shown:

```
If "%OS%" == "Windows_NT" goto SKIP
If NOT "%WINBOOTDIR%" == ""  goto 95

REM Run AVUpdate using  WIN3x syntax
net use v: \\NTSERVER_NAME\cheyupd$
v:\avupdate.exe
net use v: /d
goto SKIP
:95
REM Run AVupdate using WIN95 syntax
\\NTSERVER_NAME\cheyupd$\avupdate.exe
:SKIP
```

For the *NTSERVER_NAME* parameter, enter the name of the NT machine set up to be the distribution server. Cheyupd$ is a hidden share that InocuLAN creates on the NT machine to which the workstations will attach. (This share will be removed if the InocuLAN service is stopped or not running.)

Modify the AVUPDATE.INI file

4. Modify the AVUPDATE.INI file, if necessary.

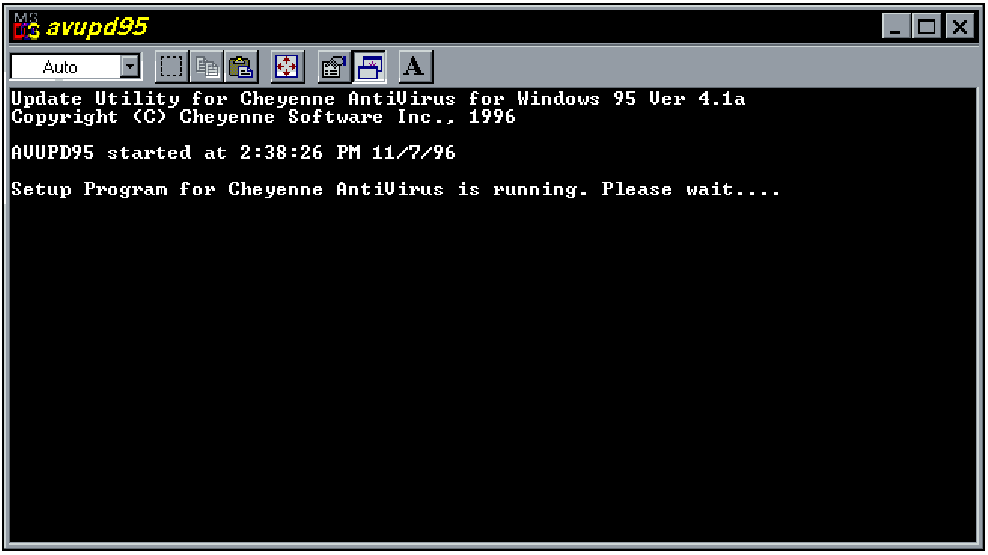
The AVUPDATE.INI file works without modification. However, to customize the install process, you may want to alter certain parameters.

Make sure the InocuLAN service is running on the NT machine. At this point, you may log in to the server and the AVUPDATE process begins.

NOTE:The first time you log in from a workstation, the installation files will have to be decompressed. This will add to the time required for the installation. All subsequent installations will be faster.

What happens on the workstation

When the user logs in to the NT workstation, the login script runs, launching AVUPDATE. A screen similar to the following appears on the workstation (with operating system specific variations):



```
Update Utility for Cheyenne AntiVirus for Windows 95 Ver 4.1a
Copyright (C) Cheyenne Software Inc., 1996

AVUPD95 started at 2:38:26 PM 11/7/96

Setup Program for Cheyenne AntiVirus is running. Please wait....
```

In Windows 95, a second window opens, showing the files being copied from the server. In Windows 3.x, all processes are seen in a single window.

All installation options run transparently, based on the AVUPDATE.INI file parameters, with no user input required.

When the file copying process completes, users need to restart their workstations to finish the installation. Upon restarting, the Cheyenne AntiVirus Real-Time Monitor begins to run, providing real-time virus protection.

For Windows 3.x users, upon their first restart after running AVUPDATE, they will receive a message asking if they wish to create an InocuLAN program group. By clicking yes, the program group is created.

Subsequent logins to the server does not re-install Cheyenne AntiVirus. AVUPDATE checks for the presence of AntiVirus on the workstation and does not install if a copy already exists.

However, if you have updated AntiVirus files on the NT server, AVUPDATE automatically updates the workstations with these new files.

Updating workstation software

The AVUPDATE program automatically updates workstations with new virus signature files as users log in to the NT server.

Signature files are automatically downloaded and placed in the correct directories through the use of the InocuLAN for Windows NT automatic download and distribution function.

To set up automatic software updating:

Run the autodownload program

1. Setup and run the InocuLAN for Windows NT automatic download and distribution, as described in the InocuLAN 4 for Windows NT Guide.

   When the download is complete and files have been released for distribution, you are ready to proceed with AVUPDATE.

Update the login script

2. Modify the login script used on the NT server by adding the following exactly as shown:

```
If "%OS%" == "Windows_NT" goto SKIP
If NOT "%WINBOOTDIR%" == ""  goto 95


REM Run AVUpdate using  WIN3x syntax
net use v: \\NTSERVER_NAME\cheyupd$
v:\avupdate.exe
net use v: /d
goto SKIP
:95
REM Run AVupdate using WIN95 syntax
\\NTSERVER_NAME\cheyupd$\avupdate.exe
```

:SKIP

For the *NTSERVER_NAME* parameter, enter the name of the NT server set up as the distribution server. Cheyupd$ is a hidden share that InocuLAN creates on the NT machine to which the workstations attach.

Modify the AVUPDATE.INI file

3. Modify the AVUPDATE.INI file, if necessary.

   The AVUPDATE.INI file works without modification. However, to customize the install process, you may want to alter certain parameters.

NOTE:For details on AVUPDATE Configuration settings for InocuLAN for NetWare, please refer to the “AVUPDATE User Guide” documentation.

4. Make sure the InocuLAN service is running on the NT machine. At this point, you may log in to the server and the AVUPDATE process will begin.

NOTE:AVUPDATE will check if the files on the server are newer than the files on the workstation. If the files are not new, no update will take place. If the files are new, AVUPDATE will automatically copy the new files onto the workstation.

5

Chapter

ALERTING USERS WHEN A VIRUS IS DETECTED

In this chapter, you will learn:

Page	
5-2 ➢	How Alert works
5-6 ➢	How to configure Alert
5-10 ➢	How to use broadcast options
5-15 ➢	How to use SNMP options
5-31 ➢	About Alert’s logs

Alert basics

What is Alert?

Alert is a notification system that sends messages from InocuLAN and other Cheyenne products to persons in your organization using different methods of communication. These messages (status, warning, and errors) can be sent to the system administrator, a hardware technician, or anyone else, in or out of the office. An individual or groups of persons in different segments of the network can also be notified.

How does Alert work with InocuLAN?

Alert does not generate its own messages. For example, InocuLAN generates warning messages whenever a virus is detected. These warning messages are passed to Alert, which sends the notification.

Alerts can be sent via:

- Broadcasts - Alert broadcasts can be sent to specific NT machines or NT domains.
- Pager - Numeric and alphanumeric messages.
- Electronic Mail - Microsoft Mail, Microsoft Exchange, and Lotus Notes.
- Trouble Tickets - An alert message can be printed through any print queue on your network.
- Simple Network Management Protocol (SNMP) managers - Such as NetWare Management System (NMS) and HP OpenView.
- Local and Remote NT Event Log Notification.

- ➢ CA-Unicenter TNG Option-Send a message to the TNG console and/or World View rtepository when an alert is generated.

In addition, Alert 4.0 features include:

- ➢ Remote Management and Configuration of Alert Service.
- ➢ Alerts from clients may now be sent using IP in addition to the standard IPX protocol.
- ➢ Messages containing full paths of the virus-ridden files.

NOTE:Alert 4.0 is also compatible with other Cheyenne products. Any configurations previously set will not be overwritten. It is recommended that you run Alert and verify your settings before running InocuLAN.

What are the components of Alert?

Alert has two basic components:

- ALERT SERVICE - This is the Service that is responsible for the reception, processing, and distribution of alert messages.
- ALERT MANAGER - This is where you can configure how Alert broadcasts its messages.

Running the Alert Manager

To view and/or modify Alert settings:

1. For Windows NT 3.51 users, double-click on the Alert Manager icon in the InocuLAN for Windows NT Group.

   For Windows NT 4.0 users, click Start, then InocuLAN, then Alert.

   The Alert Manager screen appears:

Pressing the arrow button will start the Alert Service immediately. Once the service is running, the toolbar button is grayed out. The Alert Service must be started BEFORE items can be added or edited.

Stops the Alert Service.

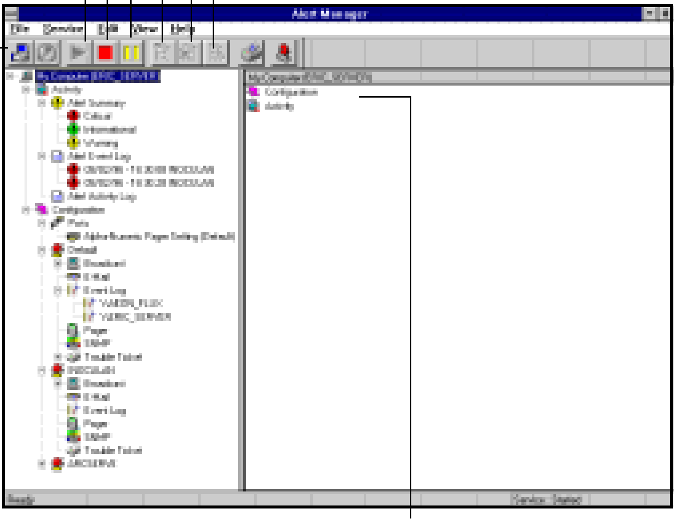
Pauses the Alert Service. You can still add/edit items.

Create a new item for the highlighted Alert mechanism.

Delete a highlighted item.

Edit a highlighted option.

Click to connect to a remote machine.



Information regarding the left-hand Function tree is displayed here.

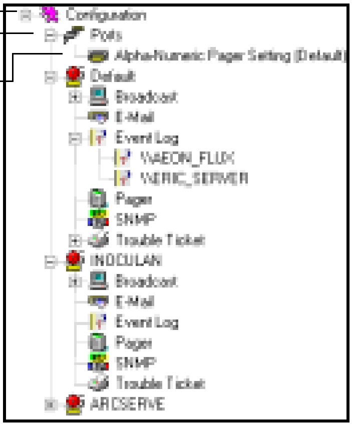
A closer look at the Alert Parameter Tree

Function Leaf Object

Option Leaf Object

Available Item(s) Object

Click on the [+] to expand the application specific recipient information. Click on [-] to collapse that part of the tree.



Configuring Alert

Alert allows for the configuration of the default settings. These settings are used by all the applications that use the Alert Service. You can also enter configuration information specifically for an individual application, which will override the default Alert configuration. Each application that uses Alert is displayed as a leaf on the left-hand function tree.

Starting the Alert Service

In order to display or configure Alert, it is necessary to start the Alert Service.

1. Click on the Alert Service tool-bar button.

   Plus signs appear under the “My Computer” leaf object once the Alert Service has been started.

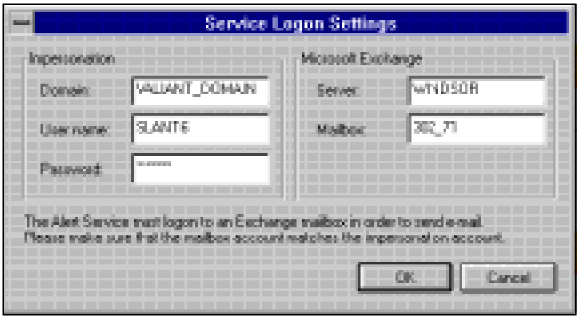
2. Click on the plus signs to expand the function and options object leaves.

Establishing a Service Account connection

The Alert Service must be able to communicate with the Windows NT server, otherwise Alerts are not sent.

An account must be created by the Windows NT Administrator that has “Log on as a Service” user rights. The domain, user name, and password for that Windows

NT account must be entered. If such a login does not exist when Alert is first started, the Service Login Settings dialog box appears.



Service Logon Settings

Impersonation

Domain: VALIANT_DOMAIN

User name: SLANT6

Password: ******

Microsoft Exchange

Server: WINDSOR

Mailbox: 302_71

The Alert Service must logon to an Exchange mailbox in order to send e-mail.
Please make sure that the mailbox account matches the impersonation account.

This will be grayed-out, unless you have installed the Microsoft Exchange client.

To login the Alert Service:

1. Pull down the Service menu and select “Set Service Account”.

NOTE:The Alert Service must be started, as shown on page 5-6, before Set Service Account can be accessed.

The Service Logon Settings dialog box is displayed.

2. Enter the Domain, User name, and password you plan to use with the Alert service.

3. If you are running the Microsoft Exchange Client, the server name and mailbox must be specified.

NOTE:This mailbox must be associated with the specified account.

4. Click on OK to save the information.

Editing and creating Port configurations

The *Ports* object, located under the Configuration object, contains communication port profiles. Port configurations are used by the Pager and any function that utilizes serial port access.

When adding a new Port object:

1. Select the “Ports” leaf object located under the “Configuration” leaf for the desired machine.

2. Right-click to display the pop-up menu and select “New Item.”

When editing a current Port configuration object:

1. Expand the “Ports” leaf object. Select the configuration you wish to edit.

2. Right-click to display the pop-up menu and select “Edit Item.”

3. Click OK when completed.

   The following fields are configured:

Port

Select the communications port being used.

Baud Rate

Select the baud rate.

Parity

Select the parity setting: NONE, ODD, or EVEN.

Data Bits

Select the number of data bits, 7 or 8.

Stop Bits

Enter the number of stop bits, 1 or 2.

NOTE: For numeric pagers, the recommended settings are: 8 data bits, NO parity, 1 stop bit. For alphanumeric pages, the recommended settings are: 7 data bits, EVEN parity, 1 stop bit. Consult the pager’s user guide if you encounter any problems with the pager communication.

Using the Broadcast option

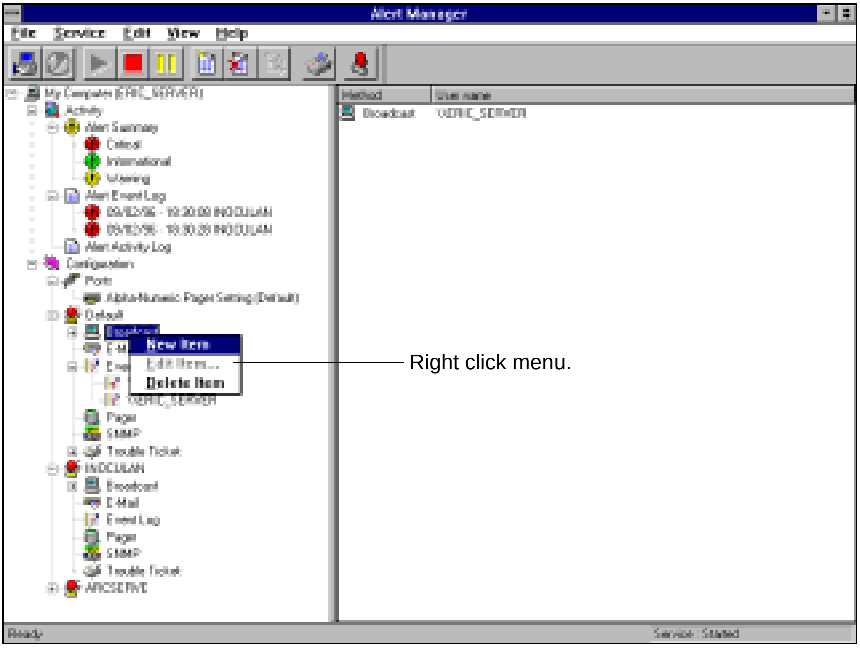
Alert broadcasts can be sent to specific network users or groups when InocuLAN detects a virus on your network.

Adding broadcast recipients

To add broadcast recipients:

1. In the Alert Manager, click the Broadcast name on the left-hand side of the screen.

2. Right-click to display the context menu and select "New Item."

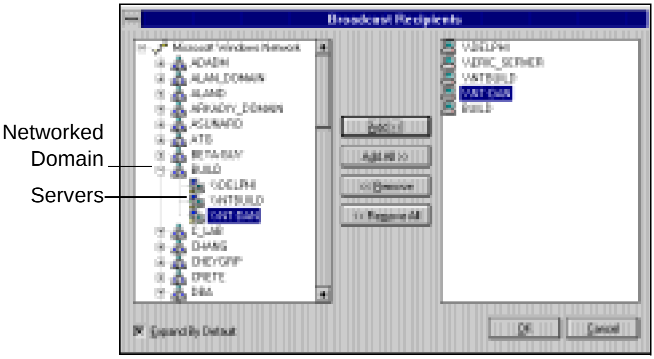


Right click menu.

The Broadcast Recipient box is displayed.

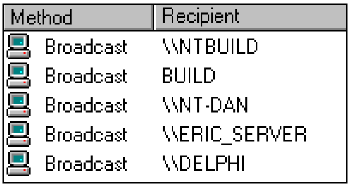
3. You can select an entire Windows NT domain or expand a domain to reveal its servers.

Select a domain or an individual server and click the Add button to add it to the recipient list.



4. Click the OK button when you have completed the broadcast recipient additions.

   The Broadcast information is displayed on the right side of the Alert main screen.



Method	Recipient
Broadcast	\\NTBUILD
Broadcast	BUILD
Broadcast	\\NT-DAN
Broadcast	\\ERIC_SERVER
Broadcast	\\DELPHI

Using the Pager option

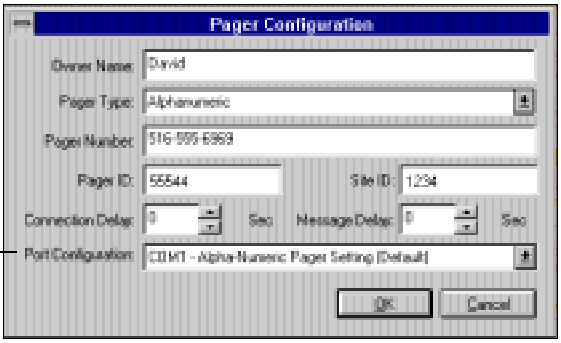
The pager option is used to a send a pager message when a virus is detected. Both numeric and alphanumeric pagers can be used at the same time.

Adding pager recipients

1. Select the “Pager” leaf object located under the “Configuration” leaf for the desired machine.

2. Right-click to display the pop-up menu and select “New Item.”

The Pager Configuration screen appears.



Owner Name: David

Pager Type: Alphanumeric

Pager Number: 516-555-6969

Pager ID: 55544 Site ID: 1234

Connection Delay: 3 Sec Message Delay: 0 Sec

Port Configuration: COM1 - Alpha-Numeric Pager Setting [Default]

The Port Configuration is set through the Ports object.

Owner name

Enter the name of the Pager Recipient.

Pager Type

Indicate if you are using a numeric or alphanumeric pager.

Pager Number

Enter a maximum of 24 characters. If a digit, such as 9, is needed for a dial tone, it must be included in this field.

A comma can be entered to indicate a one second pause. If a longer pause is desired, a string of commas can be entered.

A dash (-) can be used to separate digits, but it has no function. (Since this can vary by modem, you should verify this with your modem manual.)

Pager ID

Enter up to eight digits to identify the pager that will receive the alerts.

Site ID

Enter up to four digits to identify where the alert occurred. This ID is included in the message to the pager. Therefore, if the number is less than four digits, you should use leading zeros.

Connection Delay

Enter the number of seconds you want to wait before a connection is made with the pager company. This will vary with your pager company, location, time of day, telephone equipment, and telephone traffic. If the connection is not established immediately, adding a delay can prevent the alert from being sent before the connection is established.

Message Delay

Enter the number of seconds to wait between the time the connection is made and the alert message is sent.

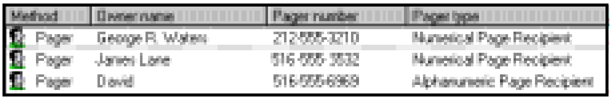
Port Configuration

Select the appropriate Port configuration from the drop down list. This configuration profile can be edited and additional pager profiles can be created. These pager configuration profiles are stored under the *Ports* leaf object.

NOTE: When sending an alphanumeric message, consult your paging service for proper modem settings. The Alert service requires the TAP protocol for alphanumeric pages.

3. Click OK to save your information.

   The pager recipients are displayed on the right side on the Alert Manager screen.



Method	Owner name	Pager number	Pager type
Pager	George R. Waters	212-555-3210	Numerical Page Recipient
Pager	James Lane	516-555-3532	Numerical Page Recipient
Pager	David	516-555-6969	Alphanumeric Page Recipient

4. Double-clicking on each recipient's name under the Pager object displays all the pager information for the selected item.

Interpreting the numeric pager message

When a numeric pager is sent because of a virus alert, the coded message will appear as: Message = DDSSSSCC

DD is the virus detection code number. It tells you which component of InocuLAN has detected a virus.

You must check InocuLAN's scanning records to determine which machine is infected and which files or directories contain the virus.

Virus Detection Code	Description
01	Real-Time Monitor detected viral activity on a local machine. Viral activity includes: Unauthorized reformatting of the hard disk, a change in the boot sector, or a change in the partition table.
02	Real-Time Monitor detected a virus in a local file.
03	A boot virus or a change to the Critical Disk Area was detected on a local machine.
04	The InocuLAN Manager detected a virus at a local machine.
05	The InocuLAN Server detected a virus on a machine.
07	Real-Time Monitor detected a virus in memory.
08	Real-Time Monitor detected a boot virus.

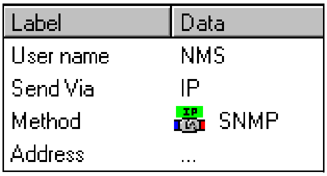
SSSS is the user defined site number from the Pager Configuration screen. The site number represents the machine that detected the virus.

CC is the user defined custom code from the Pager Configuration screen. The custom code represents the machine that sent the message.

Using the SNMP option

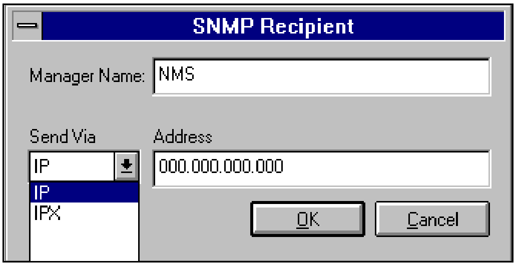
The SNMP option is used to send an SNMP 'trap' (message) to an SNMP manager when an alert is generated. Examples of SNMP managers include NetWare Management System (NMS) and HP OpenView.

1. Highlight the SNMP leaf object to display the current SNMP settings on the right-hand side.



Label	Data
User name	NMS
Send Via	IP
Method	SNMP
Address	...

2. Click on the Edit Item or New Item toolbar button (or use the right click menu) to edit/configure the SNMP recipient.



SNMP Recipient

Manager Name: NMS

Send Via: IP

Address: 000.000.000.000

3. Enter information on the SNMP Configuration screen.

Manager Name

Enter the name of the SNMP Manager.

Via IPX

Select IPX and enter the 8 byte network address of the machine where the SNMP manager is located. Next, enter the 12 byte node address of the machine where the SNMP manager is located. Use this field for Novell networks.

Via IP

Select IP and enter the IP address of the machine where the SNMP manager is located. Use this field if you are running the TCP/IP stack.

3. Click OK to save your information.

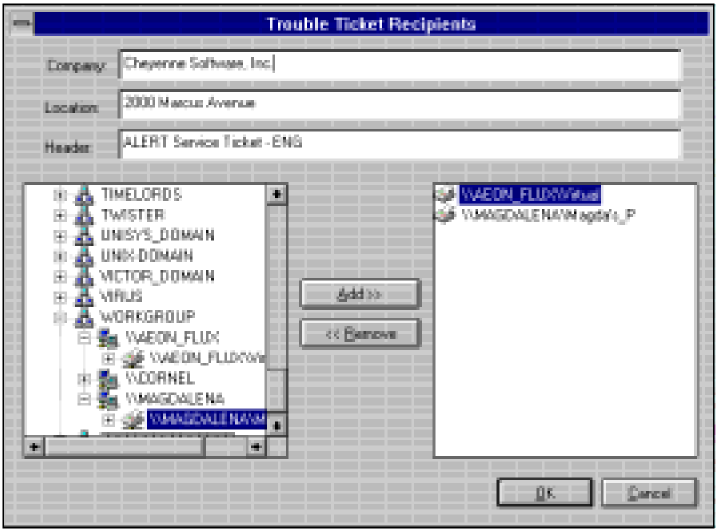
NOTE: The Management Station must be configured to receive the alert. Please consult the Release Notes for information about several SNMP managers.

Using the Trouble Ticket option

Trouble tickets are used to alert users through a printed document.

To create a Trouble Ticket:

1. Highlight the Trouble Ticket leaf object.
2. Click on the Edit Item or New Item toolbar button (or use the right-click menu).



Trouble Ticket Recipients

Company: Cheyenne Software, Inc

Location: 2000 Marcus Avenue

Header: ALERT Service Ticket - ENG

Recipient Browser.

Type in the following information into the above fields.

Company/Location

Enter the name of your company and its location.

Header

Enter the information that should appear at the top of each Trouble Ticket.

Recipient

3. Use the browser to select the printer recipient.

Highlight the chosen printer.

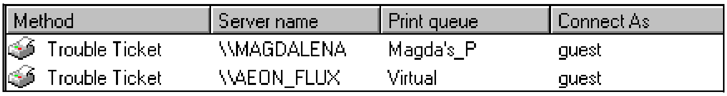
4. Click Add to move that printer on to recipient list.

   You will be prompted to provide the username and password to connect to the printer device.

5. To add additional recipients, repeat steps 3 and 4.

   Click OK to save the information.

   The information is displayed.



Method	Server name	Print queue	Connect As
Trouble Ticket	\\MAGDALENA	Magda's_P	guest
Trouble Ticket	\\AEON_FLUX	Virtual	guest

Using the E-mail option

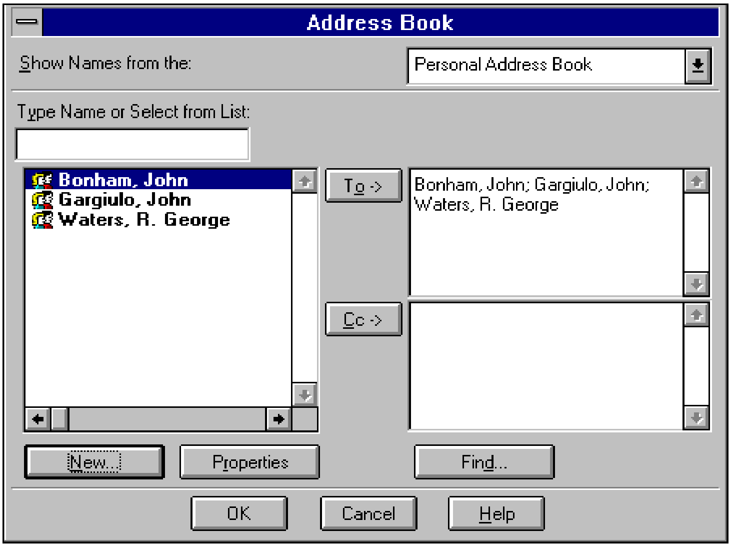
The E-mail option is used to send E-mail messages to specific users when a virus is detected. If the Microsoft Exchange Client is installed, Alert will support only the Microsoft Exchange Server.

To setup the E-mail recipients:

1. Highlight the E-Mail leaf under the INOCULAN object.

2. Click on the New Item toolbar button

   The mail login dialog box will appear:



Address Book

Show Names from the: Personal Address Book

Type Name or Select from List:

Bonham, John
Gargiulo, John
Waters, R. George

To -> Bonham, John; Gargiulo, John; Waters, R. George

3. Select the E-mail recipients using the dialog provided by the mail system.

4. Click OK to save the information.

Assigning Attachments to E-mail Messages

File attachments can be added to the E-mail messages that are sent to the selected recipients. This can be used to inform the users of what steps to take in a viruses was found.

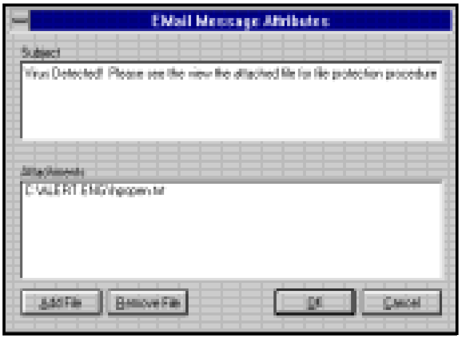
To assign attachments to the message and define a subject heading:

1. Select the E-mail leaf object.

2. Right click to display the pop-up menu.

3. Select Message Attributes.

   The message attributes box will appear:



Subject
Virus Detected! Please see the view the attached file for file protection procedure

Attachments
C:\ALERT.ENG\hgopen.txt

4. Enter a short subject heading.

5. Click on <u>A</u>dd File.

   Select the file(s) you wish to attachments and click OK.

6. Click OK to save the attachments.

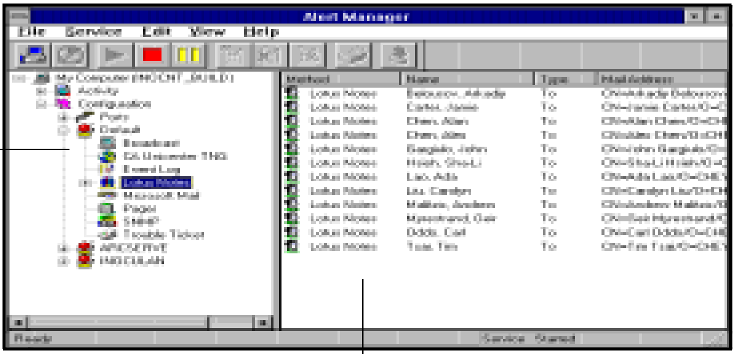
NOTE: Click on the E-mail leaf object and select Message Attributes to review or add any additional attachments.

Using the Lotus Notes Option

The Lotus Notes Option makes it possible to send a message to a Lotus Notes user when an alert is generated.

To send an Alert message to a Lotus Notes user:

1. Highlight the Lotus Notes leaf object to display the current Lotus Notes settings on the right-hand side.



Method	Name	Type	Mail Address
Lotus Notes	Belousov, Arkadiy	To	CN=Arkadiy Belousov
Lotus Notes	Carlos, Jamie	To	CN=Jamie Carlos/O=C
Lotus Notes	Chen, Allen	To	CN=Allen Chen/O=CH
Lotus Notes	Chen, Alex	To	CN=Alex Chen/O=CH
Lotus Notes	Gargiulo, John	To	CN=John Gargiulo/O=
Lotus Notes	Hsieh, Shea-Li	To	CN=Shea-Li Hsieh/O=C
Lotus Notes	Lao, Adi	To	CN=Adi Lao/O=CHEY
Lotus Notes	Liu, Carolyn	To	CN=Carolyn Liu/O=CH
Lotus Notes	Mattsson, Anders	To	CN=Anders Mattsson/O
Lotus Notes	Mjaastrand, Gair	To	CN=Gair Mjaastrand/O
Lotus Notes	Odds, Carl	To	CN=Carl Odds/O=CHE
Lotus Notes	Tsai, Tim	To	CN=Tim Tsai/O=CHEY

Highlight the Lotus Notes leaf object to display the current settings.

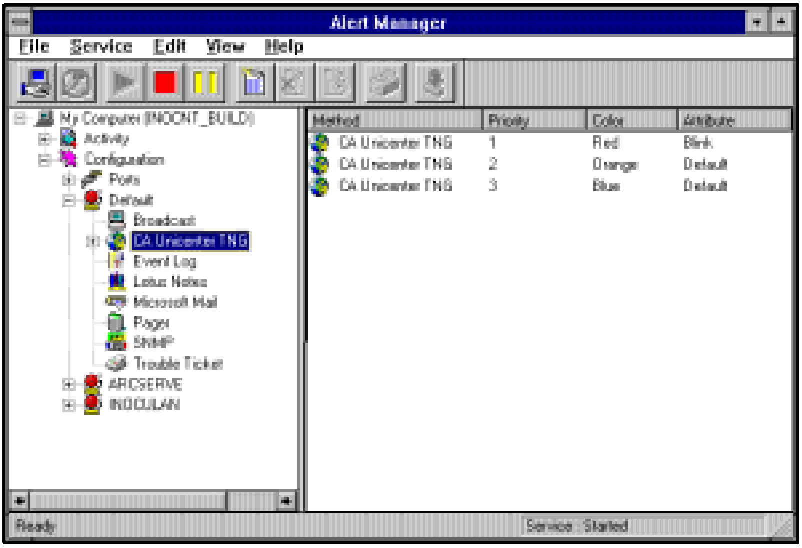
In this right-hand portion of the Alert Manager you will see the current Lotus Notes settings.

Lotus Notes Settings

To set the configuration settings for the Alert service:

2. Right click the Lotus Notes leaf object to bring up the context menu and select the Lotus Notes settings.

   The following screen appears:.



Method	Priority	Color	Attribute
CA Unicenter TNG	1	Red	Blink
CA Unicenter TNG	2	Orange	Default
CA Unicenter TNG	3	Blue	Default

3. Enter the path where Lotus Notes is installed.

4. Enter the password.

   If you want the service to switch to another User Id, check Specific account and supply the next three fields:

   ➢ Id file

   ➢ Mail Server

   ➢ Mail File

Click OK upon completion of these steps.

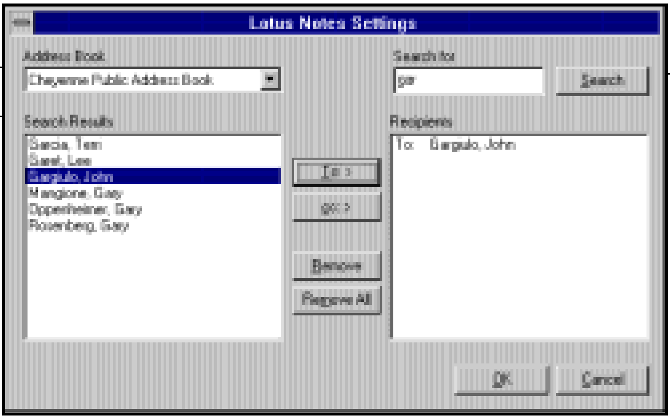
Lotus Notes Recipients

From the Alert Manager screen, click on the *Edit Item* or *New Item* toolbar button (or use the right click menu) to edit/configure the Lotus Notes recipient.

The following screen appears:

Select Address book.

Highlight user(s) from Search Results list.



Address Book: Cheyenne Public Address Book

Search for: gar

Search Results:
Garcia, Tom
Garet, Lee
Gargulo, John
Mangione, Gary
Oppenheimer, Gary
Rosenberg, Gary

Recipients:
To: Gargulo, John

Enter a value in Search for and press here.

5. Select an Address Book from the pulldown list of the Lotus Notes Settings dialog.

6. Enter a value to Search for, and then press the Search button or Enter key.

   The Search is performed on the Fullname Field of the Address book.

7. Select your prospective Lotus Notes Alert recipient from the Search Results list.

8. Select To:> or cc:> to add a user to the recipient list.

   Select Remove to remove a user.

9. Select Remove All to delete all recipients.

   Click OK upon completion of the above steps.

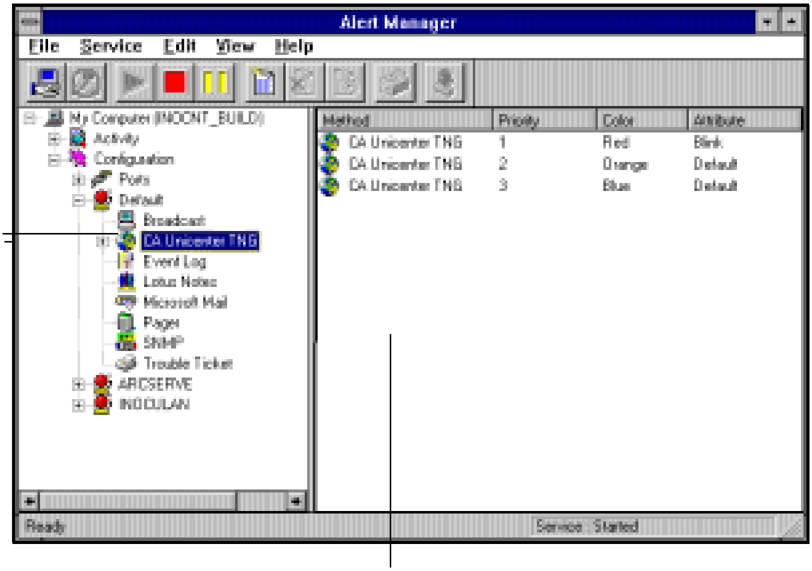
Using the CA-Unicenter TNG Option

The CA-Unicenter TNG (The Next Generation) Option makes it possible to send a message to the CA-Unicenter TNG console and/or World View repository when an alert is generated.

To send a message to the CA-Unicenter TNG Console and/or the World View repository:

1. Highlight the CA-Unicenter TNG leaf object to display the current CA-Unicenter TNG Settings on the right-hand side.

   The following screen appears:



Method	Priority	Color	Attribute
CA Unicenter TNG	1	Red	Blink
CA Unicenter TNG	2	Orange	Default
CA Unicenter TNG	3	Blue	Default

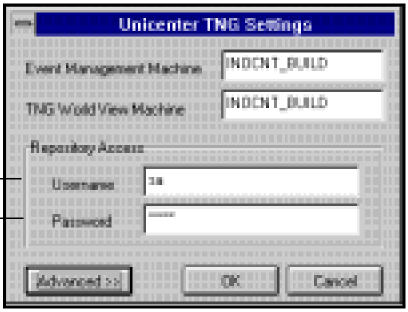
Highlight the TNG leaf object to display current TNG settings.

This portion of the Alert Manager screen displays your current TNG settings.

TNG Settings

2. Right click the CA-Unicenter TNG leaf object to bring up the context menu and select CA-Unicenter TNG Settings.

The following screen appears:



Enter Username.

Enter Password.

Unicenter TNG Settings

Event Management Machine: INDCNT_BUILD

TNG World View Machine: INDCNT_BUILD

Repository Access

Username: sa

Password: *****

3. Enter the Event Management Machine and CA-Unicenter TNG World View Machine names.

   The Event Management machine identifies the computer running the Unicenter Event Management console. The TNG World View machine identifies the computer containing the World View repository.

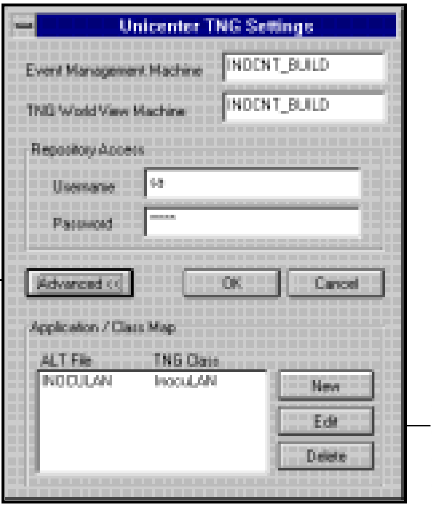
   If the World View machine is the same as the computer that you are running Alert on, enter the username and password for access to the CA-Unicenter TNG repository.

   Click on OK.

NOTE:The Alert application must be running on both the Event Management machine as well as the World View machine if specified in the Unicenter TNG settings dialog.

---

4. If you click on the Advanced button, the dialog will expand to show the following screen:



Event Management Machine: INOCNT_BUILD

TNG World View Machine: INOCNT_BUILD

Repository Access

Username: sa

Password: ******

Application / Class Map

ALT File	TNG Class
INOCULAN	InocuLAN

By selecting Advanced, the user can thereby define the class name for the application.

Mappings can be created, edited or deleted.

5. Configure Advanced Application/Class Map settings at this point.

   Application refers to the application (in this case InocuLAN) sending the alert.Class refers to the type of object (in this case InocuLAN) in CA-Unicenter TNG and is case-sensitive.

   This Advanced information is useful for those administrators familiar with the TNG repository and the definition of class types.

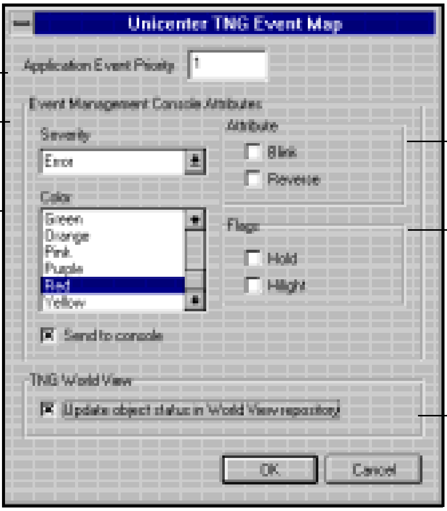
   You can now create a New mapping, Edit an existing mapping, or Delete a mapping.

   Click OK to set these changes.

TNG Recipients

6. From the Alert Manager screen, click on the Edit Item or New Item toolbar button (or use the right click menu) to edit/configure the CA-Unicenter TNG recipient.

The following screen appears:



Unicenter TNG Event Map

Application Event Priority: 1

Event Management Console Attributes

Severity: Error

Color: Green, Orange, Pink, Purple, Red (selected), Yellow

Attribute: □ Blink □ Reverse

Flags: □ Hold □ Hilight

☒ Send to console

TNG World View

☒ Update object status in World View repository

Enter priority number here.

Define Event Management Console Attributes here.

Highlight color choice of message display.

Set message to blink or reverse.

Message(s) will be held or highlighted by the console.

Update object status in World View repository.

7. Enter the Application Event Priority.

   Currently, all applications calling Alert specify an Event Priority from the following table:

ALERT SPECIFICATIONS

Events Priority	Description
1	ERROR
2	WARNING
3	INFORMATION

8. Define the settings using the Event Management Console Attributes section of the dialog.

   Within TNG you can define the attributes for the console messages received from your machine.

   Select the attributes, colors, etc., you want and check Send to console.

9. To tell Alert to search for the Application object in the TNG repository, check the Update object status box in World View repository.

   Click OK to complete these steps.

Sample TNG Alert Scenarios

If you want to send informational alerts to the CA-Unicenter TNG Console using blue text, for example, configure a recipient as follows:

Event Priority	Description
3	Application Event Priority
Blue	Color
☑	Send to Console

If you want to send error alerts to the CA-Unicenter TNG Console using red text, and have the object status in the World View repository updated, configure another recipient as follows:

Event Priority	Description
1	Application Event Priority
Red	Color
☑	Send to Console
☑	Send to World View

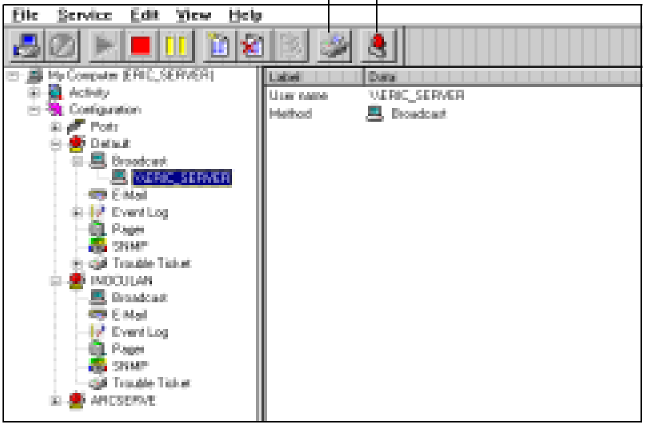
Testing the Recipients

The Test toolbar button lets you test any of the Alert messaging functions without there actually being an “alarm” condition.

You should test any features after the configuration has been completed.

To avoid unnecessary alarm, inform any Alert recipients that a test is taking place.

1. Highlight the Alert recipients.



Label	Data
User name	\\ERIC_SERVER
Method	Broadcast

Click to print data related to the selected leaf object.

Click to test.

2. Click on the test button.

The test Alert is sent to selected recipients.

Alert's Activity Log

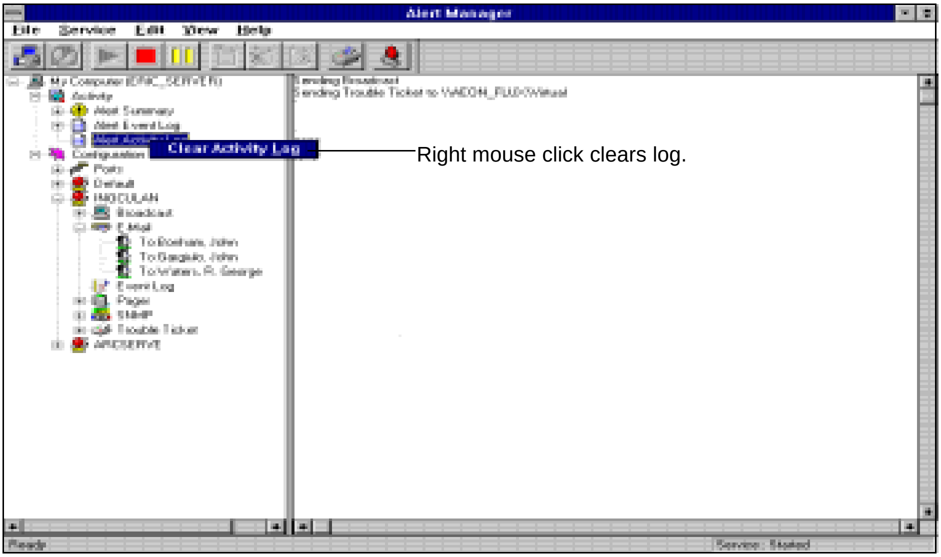
A historical listing is stored in the Activity Log. You can view, print, or clear this log.

Displaying the Activity Log

To display the Activity Log:

1. Highlight the Activity Log object from the Alert manager tree.

   The contents of the activity log are displayed in the right pane:



```
Sending Broadcast
Sending Trouble Ticket to \\AEON_FLUX\Virtual
```

Right mouse click clears log.

2. Right-click and select Clear Activity Log to delete the contents of the activity log. You might want to do this if Alert has been running for a long time and the log has grown too large.

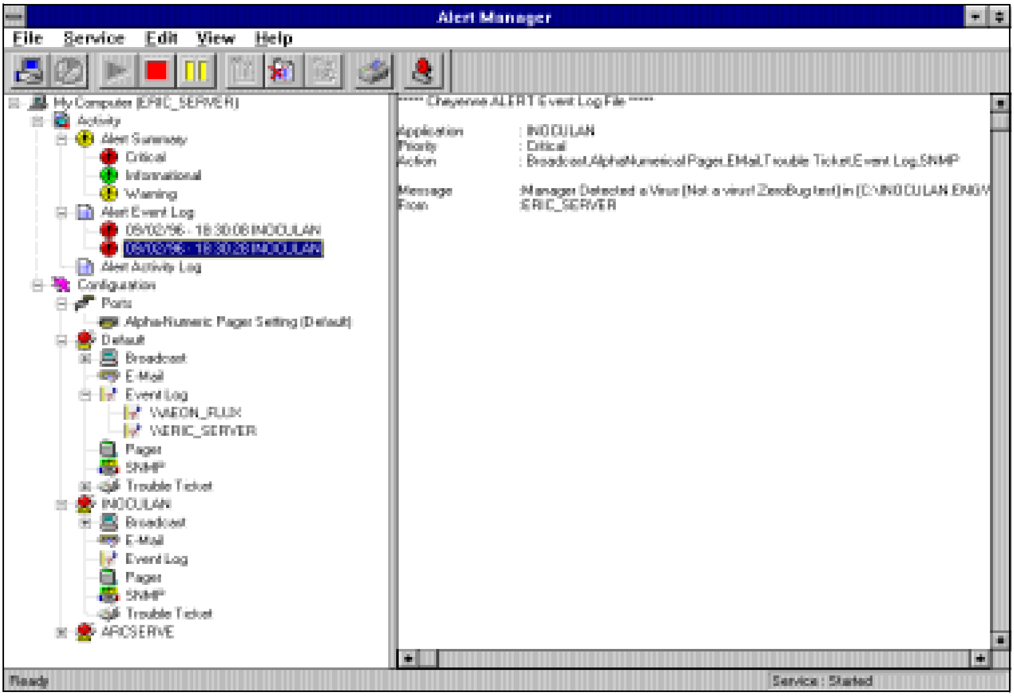
Alert's Event Log

Every message that Alert sends on behalf of all applications is stored in the Event Log. You can view, print, or clear this log.

Displaying the Event Log

To display the Event Log:

1. Highlight the Alert Event Log object. The information will appear on the right side of the screen.



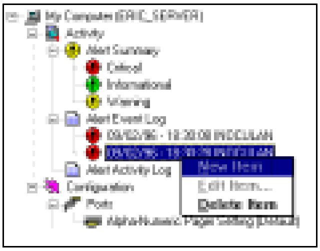
```
***** Cheyenne ALERT Event Log File *****

Application          : INOCULAN
Priority             : Critical
Action               : Broadcast,AlphaNumerical Pager,EMail,Trouble Ticket,Event Log,SNMP

Message              :Manager Detected a Virus [Not a virus! ZeroBug test] in [C:\INOCULAN.ENG\
From                 :ERIC_SERVER
```

Clearing the Messages Report Log

You can delete the Event Log. You might want to do this if Alert has been running for a long time and the log file size has grown too large.

To clear the log:

1. Highlight the Event object and right-click.



2. Select Delete Item to remove the Event Log.

Fields on the Event Log screen

Date\Time Displays the date and time the event occurred.

Description The description is determined by the applications that set the alert.

Application Tells you the application that generated the event.

Printing selected objects

Any selected leaf object’s data can be printed by selecting the *Print* command from the File menu or print button on the toolbar.

6

Chapter

SCANNING YOUR WINDOWS 95 WORKSTATION

With the Cheyenne AntiVirus for Windows 95, you can scan your workstation for viruses in Realtime, or schedule a scan job at specific intervals, keeping your system secured and virus- free at all times.

In this chapter, you will learn:

Page

6-10 ➢ Getting started with AntiVirus for Windows 95

6-11 ➢ Scanning your workstation

6-19 ➢ Using Windows 95 command line scanner

6-22 ➢ Scheduling a scan job

6-26 ➢ Using the DOS command line scanner

About Cheyenne AntiVirus for Windows 95

Cheyenne AntiVirus for Windows 95 is a powerful anti-virus solution that offers real-time virus protection and flexible scanning options to meet a variety of needs. Cheyenne AntiVirus is certified by the National Computer Security Association to detect 100% of viruses in the wild. Users will appreciate the Windows 95-style user interface, integration with the Windows 95 Explorer, and free monthly virus signature updates from Cheyenne online.

Installing AntiVirus for Windows 95

System requirements

To install and use Cheyenne AntiVirus on your Windows 95 computer, the following hardware and software requirements must be satisfied:

Machine Type	80486 DX or higher PC.
Operating System	Microsoft Windows 95
Minimum System Memory	8 Megabytes minimum, 16 megabytes recommended
Disk Space	8 Megabytes

Installation

To install Cheyenne AntiVirus for Windows 95:

1. Insert the AntiVirus Installation CD-ROM or disk 1 into the machine's drive.

2. Choose Run from the File Menu in the Windows 95 Program Manager.

   The Run dialog box opens.

3. In the Run dialog box, type **`X:SETUP`** (X is the drive containing the installation CD or diskette) and then click OK.

4. The AntiVirus Welcome Screen will appear, listing the system requirements. Click on Next to continue.

5. The License screen appears.

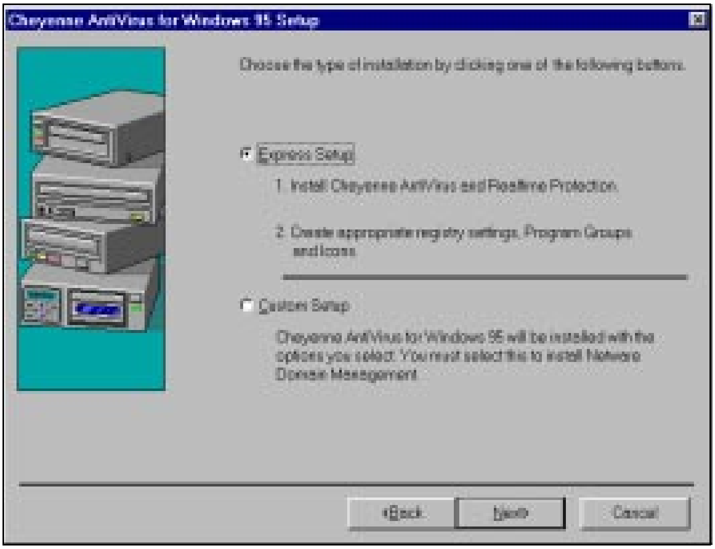
   If you are using a CD Key for licensing, enter the key in the appropriate spaces. If you are using a license file, direct AntiVirus to the file's location using the Browse button.

   Click on *Next* to continue.

6. The User Information screen appears. Enter your name and company on the screen and click on Next to continue.

7. The Select Directory screen appears. Click on Next to accept the default values, or enter a new directory and path for the installation.

8. You can choose between Express or Custom Setup. If you choose Custom, you can install NetWare Domain Manager software to enable console control of Cheyenne InocuLAN NetWare servers. However, Express install is the recommended install.



Cheyenne AntiVirus for Windows 95 Setup

Choose the type of installation by clicking one of the following buttons.

● Express Setup

1. Install Cheyenne AntiVirus and Realtime Protection.

2. Create appropriate registry settings, Program Groups and Icons.

○ Custom Setup

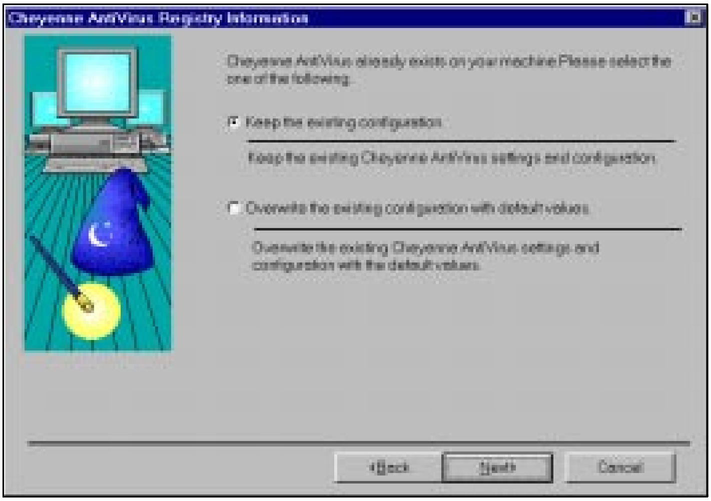
Cheyenne AntiVirus for Windows 95 will be installed with the options you select. You must select this to install Netware Domain Management.

Express setup installs all major AntiVirus components. Custom Setup allows you to choose from the following:

- Install Cheyenne AntiVirus for Windows 95 Manager
- Install Realtime Protection
- Install NetWare Domain Management Capability
- Install AutoDownload Manager

NOTE:The only way to install the NetWare Domain Management capability is through Custom Setup.

9. If you have a previous version of AntiVirus on the machine, the Registry Information screen appears.



Cheyenne AntiVirus Registry Information

Cheyenne AntiVirus already exists on your machine Please select the one of the following

● Keep the existing configuration

Keep the existing Cheyenne AntiVirus settings and configuration

○ Overwrite the existing configuration with default values

Overwrite the existing Cheyenne AntiVirus settings and configuration with the default values

If you wish to keep configuration information, choose *Keep the existing configuration.* Select this option when you just want to upgrade the new version of AntiVirus 95.

To overwrite previous information, select *Overwrite the existing configuration with default values*. This sets all values to the AntiVirus default settings.

Click on *Next* to continue.

10. AntiVirus provides automatic scanning of internet downloads. To install the internet helper applications, select the applicable browser(s) either Microsoft Internet Explorer, or Netscape browsers. Click on Next to continue.

11. A message screen notes that all necessary information has been collected. At this point, you may still click the Back button to change your installation settings.

Click *Finish* to begin the product installation.

12. AntiVirus begins copying files to your hard drive. You are prompted when the installation is complete. Restart your AntiVirus machine for all settings to take effect.

About INOCULAN.ICF

All settings for configuring INOCULAN are held within the INOCULAN.ICF file, located in the setup disk. A major advantage of this arrangement is that it allows an administrator the ability to pre-configure via the setup script file the contents of INOCULAN.ICF, thus allowing the administrator to roll out a custom configuration across his or her enterprise. The configuration includes:

- The Real-time Monitor settings
- Local Scan Settings
- Scheduled Scan Settings
- AutoDownload Settings
- Password Protection Settings

About Password Protection

By default, Cheyenne Antivirus is installed without password protection. However, the Real-time Monitor configuration may be password protected.

A password can be created/modified using the utility INSTHLPR.EXE. This can be done *before* or *after* Cheyenne AntiVirus is installed. INSTHLPR.EXE is on the setup disk but is not installed.

Before- Use INSTHLPR.EXE to create a password in the setup directory. This password can then be rolled out.

After- Copy INSTHLPR.EXE to the Cheyenne AntiVirus home directory, and run it there to create/modify the password on the current machine.

NOTE:Administrators may want to remove INSTHLPR.EXE from the setup directory when copied to a common shared place.

Uninstalling Cheyenne AntiVirus

To uninstall Cheyenne AntiVirus for Windows 95:

1. Select Uninstall from the Cheyenne AntiVirus folder in the Programs folder in the Windows 95 Start menu.

   The Cheyenne AntiVirus program is removed from your machine.

2. Reboot your system to completely remove all Cheyenne AntiVirus files from your machine.

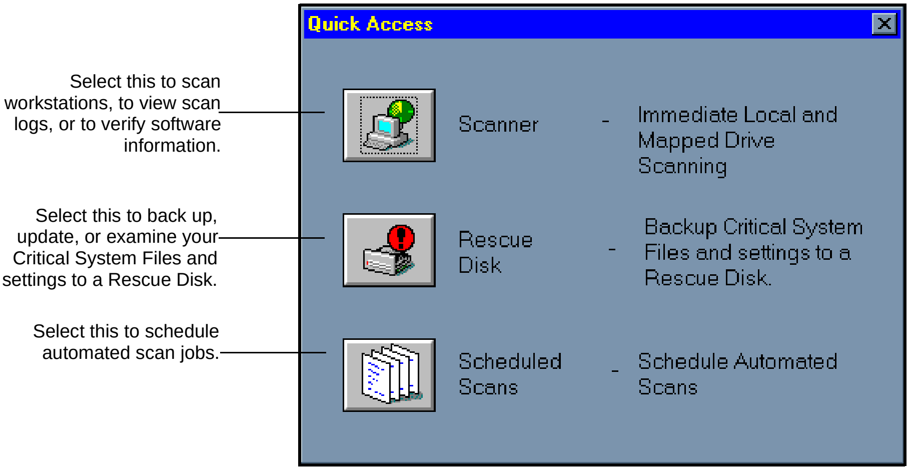
   All AntiVirus directory structures and relevant files are removed from the machine.

Getting Started with AntiVirus for Windows 95

To start Cheyenne AntiVirus for Windows 95:

1. Select the Cheyenne AntiVirus for Windows 95 program from the Windows 95 Start menu.

2. Select an option from the Quick Access dialog box/ toolbar:



Select this to scan workstations, to view scan logs, or to verify software information.

Select this to back up, update, or examine your Critical System Files and settings to a Rescue Disk.

Select this to schedule automated scan jobs.

Quick Access
Scanner
- Immediate Local and Mapped Drive Scanning
Rescue Disk
- Backup Critical System Files and settings to a Rescue Disk.
Scheduled Scans
- Schedule Automated Scans

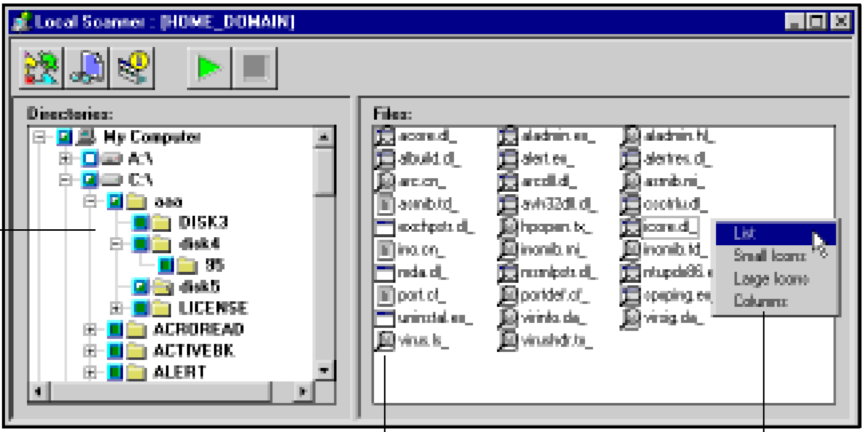
You can hide the Quick Access box through the *View/Toolbar* option on Cheyenne AntiVirus menu bar. To redisplay the Quick Access box, press F2 key at anytime.

Scanning Your Workstation

The AntiVirus scans files on your workstation, or any attached network volumes.

Follow the instructions below to scan the workstation for viruses:

1. Click the Local Scanner button to open the scanner menu:



The Explorer-style browser lets you select what to scan, right down to the individual file level.

The magnifying glass icon indicates that a file will be scanned. Click a file to change the setting, or highlight a group of files and right-click to bring up the select/deselect button.

Right-clicking in the Files window lets you change the way files are viewed, using the same options found in the Windows Explorer.

2. Select what to scan by clicking the blue marker boxes, turning them to solid green.

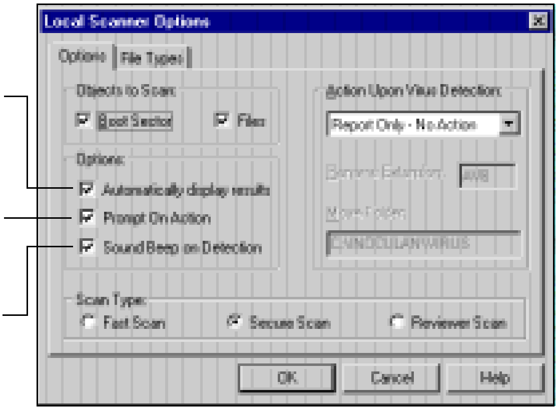
   The entire drive is automatically selected for you. You can scan this drive or you can select another.

   If you want to scan the entire drive, but you want to exclude a specific folder, click on that folder.

If you only want to scan specific files or folders, click the drive letter (to de-select everything) and then click on each file or folder you want to scan.

3. Set the scanning options by clicking on the Change Scanning Options button.

   The Local Scanner Options dialog box will appear:



Local Scanner Options

Options | File Types

Objects to Scan:
☑ Boot Sector ☑ Files

Options:
☑ Automatically display results
☑ Prompt On Action
☑ Sound Beep on Detection

Action Upon Virus Detection: Report Only - No Action

Rename Extension: AVB

Move Folder: C:\INOCULAN\VIRUS

Scan Type:
○ Fast Scan ● Secure Scan ○ Reviewer Scan

OK | Cancel | Help

Click here to see scan results as soon as the scan is finished. Otherwise, you can view results in the Scan Log.

Click here to be notified before AntiVirus takes action on infected files.

Check here for AntiVirus to beep when a virus is detected.

4. Because we want to make all scans as secure as possible, we will choose both Boot Sector and Files in the Objects to Scan field.

Scanning actions

5. You decide what to do with an infected file by choosing the correct AntiVirus action in the Action Upon Virus Detection field.

   - Because you want to decide whether or not a file is cured on an individual basis, you can choose the *Broadcast - No Action* option.
   - If you prefer that an infected file be deleted automatically, choose *Delete File* action.
   - *Cure Files* removes viruses from infected files and restores the files to their original state. If the file cannot be cured, it will be renamed with an AVB extension (refer to ‘Rename File’ below). Even if AntiVirus does cure the file, we

still recommend you to delete the infected file and then restore the original file from a backup copy or the original product installation disks.

- *Rename File* will rename the infected files by giving them an AVB extension. AVB files will not be scanned by AntiVirus. Infected files with the same name will be given incremental extensions in the form AV#, for example: FILE.AV0, FILE.AV1, etc.
- *Move File* moves an infected file from its current directory to the ANTIVIRUS\VIRUS directory.
- *Purge File* deletes an infected file so that it cannot be recovered.
- *Rename and Move File* renames infected files by giving them an AVB extension and then moving them to the ANTIVIRUS\VIRUS directory.

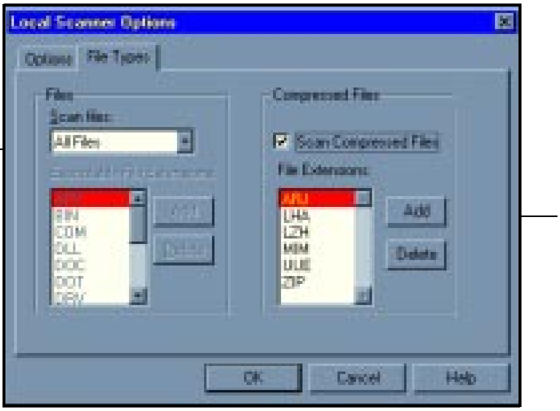
Scan Type

6. The level of scanning is set in the Scan Type field. Because you want to ensure that the files are scanned in their entirety, you choose Secure Scan. Fast Scan runs faster than Secure Scan checking only the beginning and the end of each data file. The beginning and the end of the file is where most viruses hide. Fast Scan improve scanning speed when processing large groups of data files, but it is possible for a file to have a virus that is missed by Fast Scan option.

   If you suspect you have a virus but Secure Scan is not detecting one, you can use the *Reviewer Scan* option. The Reviewer Scan can also detect viruses that are inactive or have been deliberately modified, such as in a virus testing laboratory. Note that in unique circumstances, Reviewer Scan can generate a false alarm. If you are using Reviewer Scan as your standard scanning option, you should use the *Report Only* option when you hit a virus.

Selecting files to scan

7. Now that the scanning options are set, you have to select the types of files you will scan. Click on the Files menu tab.



Scan files: All Files

☑ Scan Compressed Files

AntiVirus can scan all files, or you can include or exclude selected file types. You can also add and/or delete file types from the default list.

If the compressed file name extensions have been changed, you can add the new extensions here.

Scan Compressed file

8. Cheyenne AntiVirus can decompress PKZIP,ARJ,LHA, LZH, MIME, and UUEncoded formatted files, as well as Microsoft compressed files. Please select the extensions of the files for Antivirus to try to decompress.

NOTE:If a virus has been found, you must first decompress it and then cure the non-compressed infected file(s).

Start ▶

Stop ■

9. Click OK to accept the settings.

10. Click the Start/Continue Scanning Drive button. The scan begins immediately. Scanning job progress can be viewed in the Local Scanner window.

When the scan begins, the Start button changes from green to grey, and the Stop button next to it turns to red. To stop scanning at any point, click the Stop button.

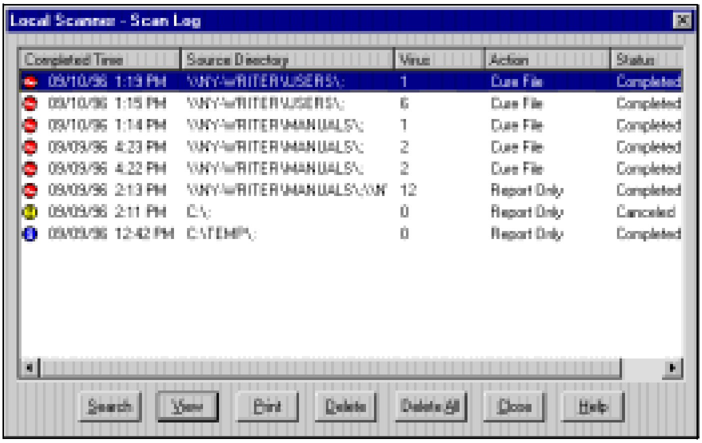
11. When the scan is completed, the Virus Scan Results window displays scanning information, including the name and location of any viruses that were found.

Checking the results of your scan

If you have the option *Automatically Display Results* selected, the results of your scan appears on the menu screen when the scan operation is completed.

If you do not have this option selected, or if you want to view the results at a later time, follow the instructions below:

1. Click the Scan Log button. The Local Scanner Scan Log menu appears as such:



Local Scanner - Scan Log

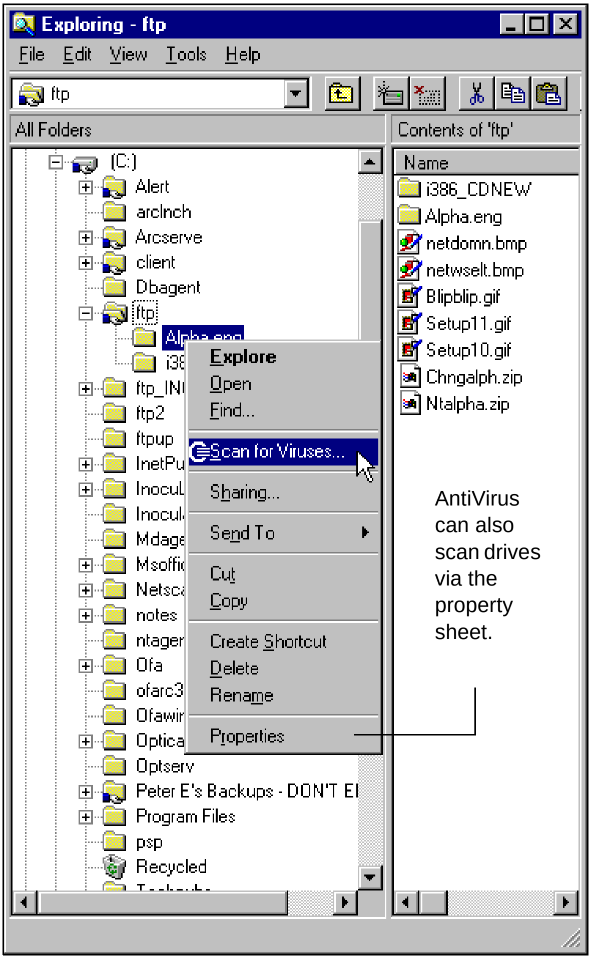
Completed Time	Source Directory	Virus	Action	Status
● 09/10/96 1:19 PM	\\NY-WRITER\USERS\:	1	Cure File	Completed
● 09/10/96 1:15 PM	\\NY-WRITER\USERS\:	6	Cure File	Completed
● 09/10/96 1:14 PM	\\NY-WRITER\MANUALS\:	1	Cure File	Completed
● 09/09/96 4:23 PM	\\NY-WRITER\MANUALS\:	2	Cure File	Completed
● 09/09/96 4:22 PM	\\NY-WRITER\MANUALS\:	2	Cure File	Completed
● 09/09/96 2:13 PM	\\NY-WRITER\MANUALS\:\W	12	Report Only	Completed
● 09/09/96 2:11 PM	C:\:	0	Report Only	Canceled
● 09/09/96 12:42 PM	C:\TEMP\:	0	Report Only	Completed

2. Highlight the job you want to find out more information about.

3. Click View or double-click on the job to view details of the scan job.

Windows 95 Enhancement - Local Scanning shell extensions

If you are using Windows 95, you can scan a directory or file by using AntiVirus shell extensions.



AntiVirus can also scan drives via the property sheet.

To use the shell extensions, locate a directory or file in My Computer or the Windows Explorer. Right-click on the directory or file and select *Scan for Viruses...*, as shown at the left.

This opens the AntiVirus shell scanner. The shell scanner uses the same scanning engine and has the same functionality as the Local Scanner. To set the scanning options, click *Advanced*. (For information on scanning options, see section *How to use the Local Scanner.* Click Start to begin the scan.

Scan progress will be shown by a moving progress bar. Scan reports are sent to the Log and can be reviewed there.

Scanning Mapped Drives

To scan a mapped, or networked drive:

1. Mark the target volume, directory, or file to scan.

2. Click on the Run button.

NOTE: A scan job running from the workstation Targeting a server volume will slow down the performance of the servers due to more disk intensive operations. For the server volumes to be properly scanned, you should use the Cheyenne InocuLAN AntiVirus software Enterprise Edition.

3. Select the options you want to include with the scanning job.

Using the Windows 95 command line scanner

The Shell Extension can be run directly from the Windows 95 command line.

The command syntax follows:

```
Inocucmd95 path option
```

For *path*, enter one of the following:

Path Statement	Description
DRIVE:\	Scans only the specified drive, such as C:\, or enter * to scan all local drives.
DRIVE:\FOLDER	Scans only the drive or drive\folder combination specified. For example, to scan the BIN folder on the C drive, enter C:\BIN.

If you are using Windows 95 long file names for a folder, the path must be contained in quotation marks. For example:

“C:\program files\cheyenne\AntiVirus” *options*

The *option* choices are explained below, by category. You can use one option or a combination of options.

What to scan

Option	Description
/EXA	Examines only the boot sector for viruses.
/EXE	Scans executable files only.

Scan method

Option	Description
/FST	Checks just the beginning and end of each data file. Using Fast Scan improves scanning efficiency when processing large groups of files. *However, it is possible for a data file to have a virus that will be missed by Fast Scan*. This option only applies to data files. Other types of files (*.EXE, *.COM, etc.) are always fully scanned.
/SEC	Examines the entire file. This is a thorough way to check files but is slower than running a fast scan.
/REV	Also examines the entire file. In addition, it searches for *virus-like* activity within files. Under unique circumstances, the Reviewer Scan may generate a false alarm. Therefore, use this scan only when the *Report Only - No Action* option is selected. You should use the Reviewer Scan to confirm the presence of a virus after a Fast or Secure scan has located a virus.

Help option

Option	Description
/HEL or /?	Displays help menu.

Interface options

Option	Description
/Q	No user interface is displayed. A message about any viruses found will be displayed at the end of the scan.
/START	Starts the scan immediately.
/MIN	Starts the scan immediately and runs in minimized form.

Action upon virus detection

Option	Description
/NOA	Scans files and reports any viruses detected. No other action is taken.
/DEL	Deletes an infected file from your workstation.
/CUR	Removes certain known viruses from infected files and restores the files to their original state. If the file cannot be cured, it will be renamed with an .AVB extension (refer to /REN below). Even if Cheyenne AntiVirus cures the file, we recommend you purge the infected file and then restore the original file.

Option	Description
/REN	Renames infected files by giving them an extension of .AVB. Files with this extension are not scanned. If a file exists with the .AVB extension and an infected file in the same folder results in the same file name, the .AVB extension is changed. The extension becomes .AV# and the number is incremented for each subsequent occurrence (.AV0, .AV1, etc.). For example, an infected MOUSE.COM is renamed MOUSE.AVB and then an infected MOUSE.SYS is renamed to MOUSE.AV0.
/MOV	Moves an infected file from its current folder to the *Cheyenne AntiVirus_home_folder*\VIRUS folder.
/PUR	Deletes an infected file so that it cannot be recovered (for example, using the Restore command in the Windows 95 Recycle Bin).
/M&R	Renames infected files by giving them a different extension and then moves them to the *Cheyenne AntiVirus_home_folder*\VIRUS folder.

Scheduling a scan job

Cheyenne AntiVirus for Windows 95 allows you to schedule scan jobs to run unattended. The Scheduled Scans menu is similar to a printer queue on the network. You can configure jobs with different options and schedule them to run at various time intervals. The following is an example on how to schedule your first scan job.

How to Schedule Scan Jobs

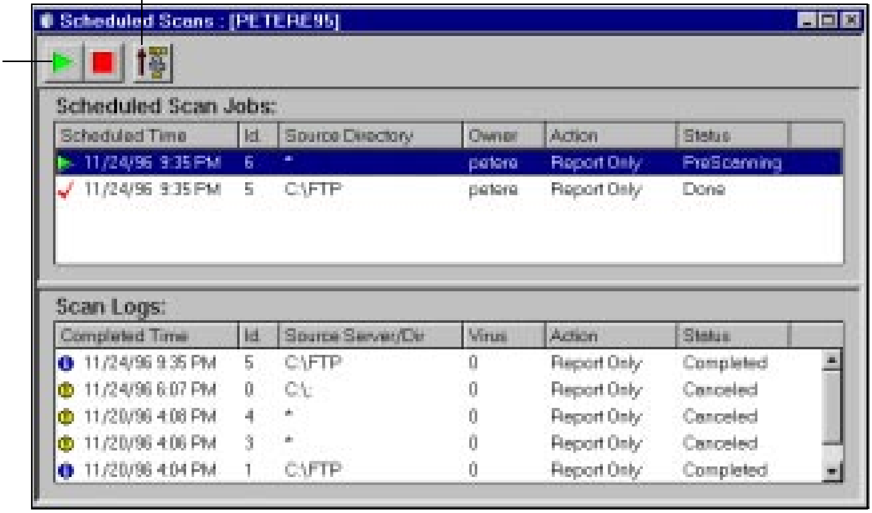
To begin the Scheduling program:

1. Click on the Scheduled Scans icon from the Quick Access menu, or go to the menu bar and select View and then select Scheduled Scans.

   Once selected, the Scheduled Scans window appears:

This button allows you to schedule regular virus signature updates from a Windows NT computer. Just click, and fill in the field information, such as time intervals, login procedures, and the manager will update the signature files automatically.

When a scan job is running, you can double click on it to view the scan progress.



Scheduled Scans : [PETERE95]

Scheduled Scan Jobs:

Scheduled Time	Id	Source Directory	Owner	Action	Status
11/24/96 9:35 PM	6	*	petere	Report Only	PreScanning
✓ 11/24/96 9:35 PM	5	C:\FTP	petere	Report Only	Done

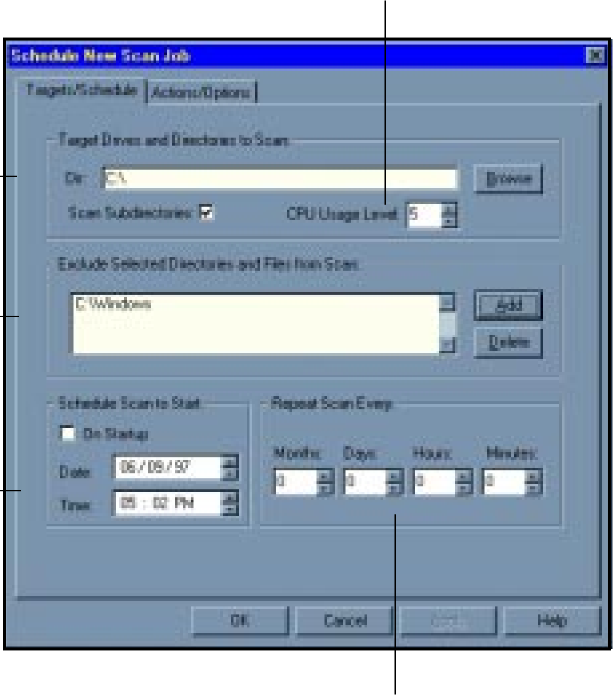
Scan Logs:

Completed Time	Id	Source Server/Dir	Virus	Action	Status
11/24/96 9:35 PM	5	C:\FTP	0	Report Only	Completed
11/24/96 6:07 PM	0	C:\	0	Report Only	Canceled
11/20/96 4:08 PM	4	*	0	Report Only	Canceled
11/20/96 4:06 PM	3	*	0	Report Only	Canceled
11/20/96 4:04 PM	1	C:\FTP	0	Report Only	Completed

2. To submit a scan job, you can select Schedule from the menu bar and then select Schedule Job.

This brings up the Schedule New Scan job configuration screen:

You can even set the level of CPU usage of the Scan job.



Schedule New Scan Job

Targets/Schedule | Actions/Options

Target Drives and Directories to Scan

Dir: C:\

Scan Subdirectories: ☑

CPU Usage Level: 5

Exclude Selected Directories and Files from Scan

C:\Windows

Schedule Scan to Start

□ On Startup

Date: 06 / 09 / 97

Time: 05 : 02 PM

Repeat Scan Every

Months: 0

Days: 0

Hours: 0

Minutes: 0

You set the files or directories that needs to be scanned.

You can choose to exclude certain directories to be excluded from the scheduled scan job.

You set the date and time of the scan job.

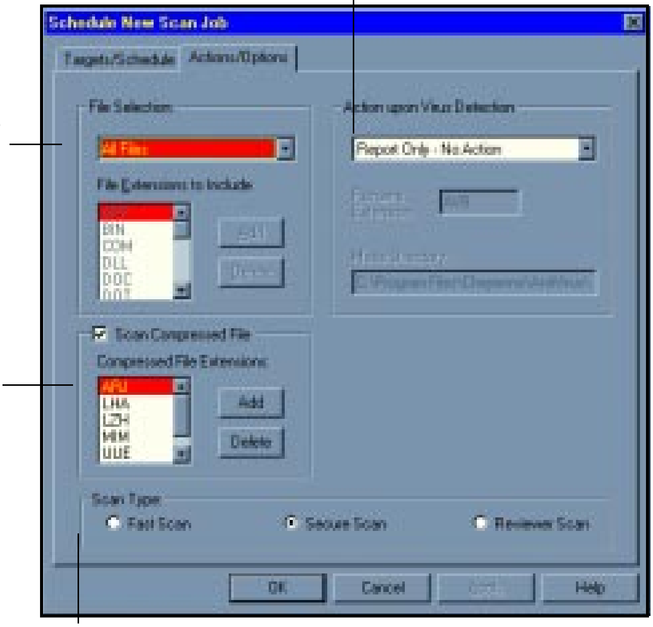
You can set the repeating interval of the scan job.

3. The second tab menu of the Scheduled Scan program is the Actions/Options tab.

   This menu is where you’ll be setting the different options or file formats, such as compression.

The Actions/Options menu appears:

You can select the different Scan Action to be taken upon virus detection.



Schedule New Scan Job

Targets/Schedule | Actions/Options

File Selection: All Files

File Extensions to Include: BIN, COM, DLL, DOC, DOT

Action upon Virus Detection: Report Only - No Action

☑ Scan Compressed File

Compressed File Extensions: ARJ, LHA, LZH, MIM, UUE

Scan Type: ○ Fast Scan ● Secure Scan ○ Reviewer Scan

You can add or exclude certain types of files.

You can add or exclude the various compressed files.

Select the type of scan job you want the scheduler to perform.

For specific Action or Option function descriptions, see “Scanning your Workstation” on page 6-11.

NOTE:The Scheduled Scan is a <u>local</u> queue. To manage queue jobs on the server level, you must use the domain managers or the managers on the InocuLAN servers.

Once the scan job has been configured, you can pull up the Scheduled Scan menu at any time to view the different type of scan jobs. Double-clicking on a specific job allows you to modify existing jobs.

Using the DOS command line scanner

Cheyenne AntiVirus for Windows 95 gives you the flexibility to enter scanning commands from the MS-DOS command line. You must be in the Cheyenne AntiVirus home directory before starting.

DOS command line syntax can be added to your AUTOEXEC.BAT file, allowing you to automatically scan your drive(s) every time you reboot your machine.

Scan results will appear on screen during the course of the scan, and will also be saved in the scan log for viewing or printing at a later time.

The command syntax follows:

```
INOCUCMD path option
```

For *path*, enter one of the following:

Path Statement	Description
DRIVE:\	Scans only the specified drive, such as C:\, or enter * to scan all local drives.
DRIVE:\FOLDER	Scans only the drive or drive\folder combination specified. For example, to scan the BIN folder on the C drive, enter C:\BIN.
SERVER_NAME	Scans all the volumes on the named server.
SERVER/VOL:	Scans the named volume only on the named server. For example, to scan the PAYROLL volume on the ACCNTG server, enter ACCNTG/PAYROLL:

If you are using Windows 95 long file names for a folder, the path must be contained in quotation marks. For example:

“C:\program files\cheyenne\AntiVirus”

The *option* choices are explained below, by category.

What to scan

Option	Description
/EXE	Scan executable files only.
/NOS	Does not scan subdirectories under the main directory.
/UPM	Scans memory up to 1M for viruses.

Scan method

Option	Description
/FST	Checks just the beginning and end of each data file. Using Fast Scan improves scanning efficiency when processing large groups of files. *However, it is possible for a data file to have a virus that will be missed by Fast Scan*. This option only applies to data files. Other types of files (*.EXE, *.COM, etc.) are always fully scanned.
/SEC	Examines the entire file. This is a thorough way to check files but is slower than running a fast scan.

Option	Description
/REV	Also examines the entire file. In addition, it searches for *virus-like* activity within files. Under unique circumstances, the Reviewer Scan may generate a false alarm. Therefore, use this scan only when the *Report Only - No Action* option is selected. You should use the Reviewer Scan to confirm the presence of a virus after a Fast or Secure scan has located a virus.

Action upon virus detection

Option	Description
/DEL	Deletes an infected file from your workstation.
/CUR	Removes certain known viruses from infected files and restores the files to their original state. If the file cannot be cured, it will be renamed with an .AVB extension (refer to /REN below). Even if Cheyenne AntiVirus cures the file, we recommend you purge the infected file and then restore the original file.
/REN	Renames infected files by giving them an extension of .AVB. Files with this extension will not be scanned. If a file exists with the .AVB extension and an infected file in the same folder will result in the same file name, the .AVB extension will be changed. The extension will become .AV# and the number will be incremented for each subsequent occurrence (.AV0, .AV1, etc.). For example, an infected MOUSE.COM is renamed MOUSE.AVB and then an infected MOUSE.SYS is renamed to MOUSE.AV0.

Option	Description
/MOV	Moves an infected file from its current folder to the *Cheyenne AntiVirus_home_folder*\VIRUS folder.
/PUR	Deletes an infected file so that it cannot be recovered (for example, using the Restore command in the Windows 95 Recycle Bin).
/M&R	Renames infected files by giving them a different extension and then moves them to the *Cheyenne AntiVirus_home_folder*\VIRUS folder.

Help option

Option	Description
/HEL or /?	Displays help menu.

Reporting options

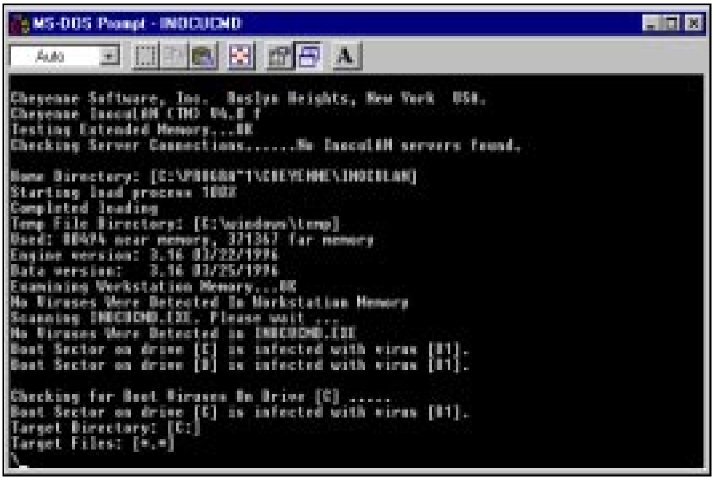
Option	Description
/LIS <report file name>	Generates a scanning report file using the specified name.
/APPend	Appends the scanning report to any previously created scanning reports.

Critical Disk Area options

Option	Description
/BAK <destination path>	Backs up the Critical Disk Area to the file specified in the path.

Option	Description
/RES <source path>	Restores the Critical Disk Area using the source file specified in the path.
/EXM <backup path>	Examines the Critical Disk Area. To compare to a previously backed up version, enter a path where it can be found.

After entering the command, messages about the progress of the scan appears in the MS-DOS window, as shown below:



```
Cheyenne Software, Inc.  Roslyn Heights, New York  USA.
Cheyenne InocuLAN (TM) V4.0 f
Testing Extended Memory...OK
Checking Server Connections......No InocuLAN servers found.

Home Directory: [C:\PROGRA~1\CHEYENNE\INOCULAN]
Starting load process 100%
Completed loading
Temp File Directory: [C:\windows\temp]
Used: 80494 near memory, 371367 far memory
Engine version: 3.16 03/22/1996
Data version:   3.16 03/25/1996
Examining Workstation Memory...OK
No Viruses Were Detected In Workstation Memory
Scanning INOCUCMD.EXE. Please wait ...
No Viruses Were Detected in INOCUCMD.EXE
Boot Sector on drive [C] is infected with virus [B1].
Boot Sector on drive [D] is infected with virus [B1].

Checking for Boot Viruses On Drive [C] ......
Boot Sector on drive [C] is infected with virus [B1].
Target Directory: [C:]
Target Files: [*.*]
\
```

Stopping a scan

You can stop the scan at any point by pressing the ESC key. This will pause the scan and present a message asking if you wish to stop scanning. Enter Y to stop the scan, or N to continue.

7

Chapter

SAFEGUARDING WINDOWS 95 WORKSTATIONS

An integral part of safeguarding your workstations is preventing viruses from gaining access to your workstation in the first place. Here are some preventive measures you can take.

In this chapter, you will learn:

Page

7-3 ➢ How to keep your workstation virus-free

7-14 ➢ How Rescue Disk protects critical disk areas

7-19 ➢ What to do if you discover a virus on your workstation

7-23 ➢ AntiVirus signature file virus listings

7-24 ➢ How to use the AutoDownload Manager

Keeping your workstation virus-free

While you can use Cheyenne AntiVirus to detect and cure problems caused by viruses, the best way to keep your workstation virus-free is to prevent viruses from gaining access to your workstation in the first place.

Cheyenne AntiVirus features

Cheyenne AntiVirus offers many features that provide a solid barrier against viruses. Detailed information about each feature can be found in this chapter.

- ➢ Real-time Monitor - Real-time-Monitor scans files as they enter or exit your workstation to and from other computers on your network. As part of Cheyenne AntiVirus's real-time protection, the Real-time-Monitor program scans for viruses each time a file is executed, accessed, or opened. Password Protection and a Temporary Bypass feature allow administrators more flexibility and control in configuring Cheyenne Antivirus to suit their enterprises.
- ➢ Rescue Disk Protection - Backing up your critical disk areas with Rescue Disk can safeguard your workstation's integrity if a virus corrupts original system boot information. Rescue Disk provides a mechanism to automatically back up the critical system files and settings required to boot your machine.The information backed up includes the master boot sector, partition table, CMOS RAM information, and

system files. Thus, Rescue Disk safeguards all the vital system information.

General suggestions

In addition to all of Cheyenne AntiVirus's features, we offer the following general suggestions to help keep your workstation virus-free:

- Set all of your executable files as Read Only files. This will reduce the chance of executable files becoming infected with viruses. Applying the Read Only file attribute to the executable will prevent most viruses from attaching, or replicating themselves.
- Use Cheyenne AntiVirus to scan floppy diskettes for viruses before copying any files from them. Even an original install of a software you just purchased from the computer store may still contain dangerous viruses.
- Always make backup copies of valuable data files, or installation diskettes. In situations where a new virus is detected, even with no cure for the virus, you can still restore a virus-free copy of the original files.

Using the Real-time-Monitor

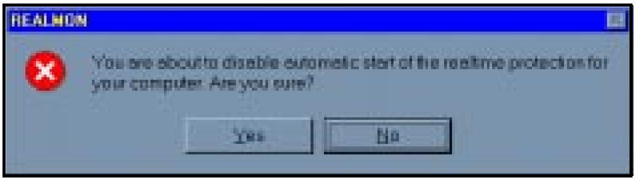
The Real-time Monitor program is a VxD (Virtual Device Driver) program that scans files on your workstation for viruses each time a file is executed, accessed, or opened. It also monitors your workstation for virus-like behavior, such as unauthorized formatting of your hard disk. Real-time Monitor can detect known and unknown viruses.

You can configure the Real-time Monitor to specify how it detects viruses and what action is takes upon detection. In addition, administrators can enable Password Protection and a Temporary Bypass feature to permit administrators more control and flexibility when rolling out Cheyenne Antivirus for Windows 95 in your workplace.

Automatic Loading of the Real-time Monitor

When Cheyenne AntiVirus was installed on your workstation, the Real-time Monitor was configured as well. The Real-time Monitor will be loaded each time the workstation is booted. You will see its icon in the Windows 95 system tray.

To prevent the Real-time Monitor from loading, you can choose to disengage it. To do so, right click on the Real-time Monitor and *uncheck* Run On Startup. You will be prompted:



You are about to disable automatic start of the realtime protection for your computer. Are you sure?

Configuring the Real-time Monitor

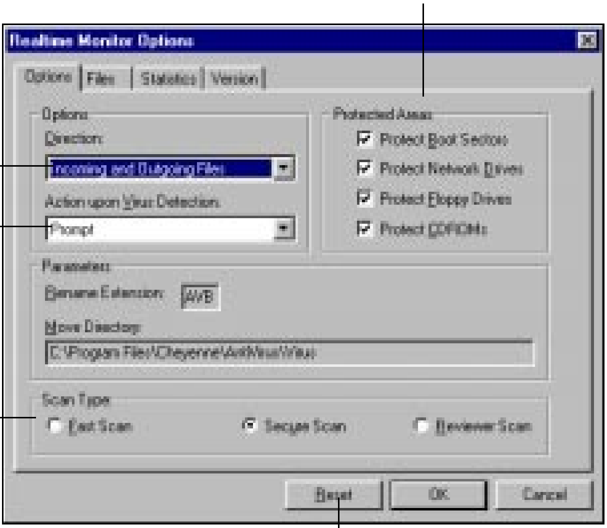
You can configure the Real-time Monitor using the Real-time Monitor's Active Window Monitor.

To open the Real-time Monitor:

1. Double-click the Real-time Monitor icon in the Windows 95 system tray.

   The Real-time Monitor Options window opens:

Check below the choices you wish to designate as Protected Areas.



Options

Direction: Incoming and Outgoing Files

Action upon Virus Detection: Prompt

Protected Areas

☑ Protect Boot Sectors

☑ Protect Network Drives

☑ Protect Floppy Drives

☑ Protect CDROMs

Parameters

Rename Extension: AVB

Move Directory: C:\Program Files\Cheyenne\AntiVirus\Virus

Scan Type

○ Fast Scan ● Secure Scan ○ Reviewer Scan

Click here to enable or disable Incoming or Outgoing Files.

Click here to select Actions to take upon Virus Detection.

Click here to specify the types of scans you wish to run.

Click here to reset the default settings.

To disable the Real-time Monitor:

1. From the Real-time Monitor Options Direction pull-down menu, click on Disable.

Click on the pull-down menu again to re-enable the Real-time Monitor.

You can also perform enable and disable functions by right clicking on the Real-time Monitor icon and highlighting your choice.

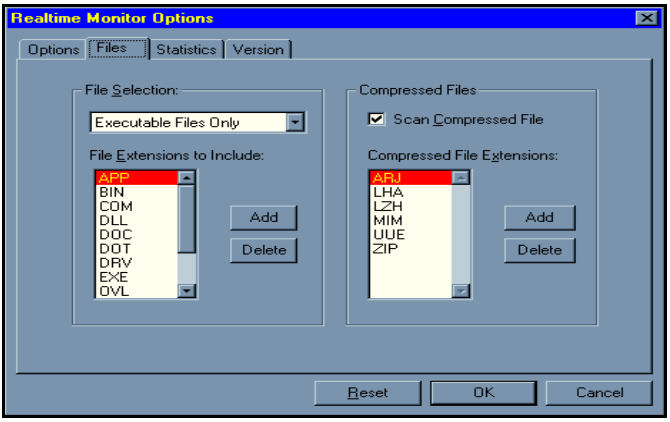
NOTE: You can re-establish the default settings of any Real-time Monitor Options screen by clicking Reset.

To specify the types of scans:

1. Choose the scan type you want from the Options menu of the Real-time Monitor window. You have three choices:
   - ➢ Fast Scan-In this type of scan, files are searched only at the beginning and end of the file, where viruses tend to be attached.
   - ➢ Secure Scan- This is the default setting. With Secure Scan, a search of the entire file is conducted.
   - ➢ Reviewer Scan- This type of scan is the most thorough and, therefore, the slowest. It searches for anything virus-like; hunting for dormant viruses, deliberately modified viruses, any virus-like behaviors. Reviewer Scan should be used when there is evidence of infection but Secure Scan does not detect any viruses.

To specify the types of files to scan:

1. Choose Files from the Options menu on the Real-time Monitor window. The following screen appears:



File Selection: Executable Files Only

File Extensions to Include: APP, BIN, COM, DLL, DOC, DOT, DRV, EXE, OVL

Compressed Files

☑ Scan Compressed File

Compressed File Extensions: ARJ, LHA, LZH, MIM, UUE, ZIP

2. From the pull-down menu, choose the File Selection: you want.

   Executable Files Only is the default option. You can deselect it to choose *All Files* or *Exclude File Extensions*.

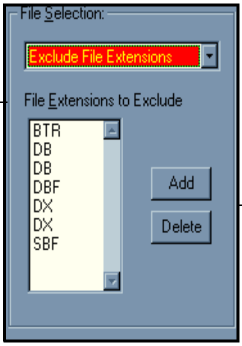
3. To add or delete specific file extensions, highlight the extension(s) you want from the scroll-bar under File Extensions to Include: and then press Add or Delete.

NOTE: When you enable File Extensions, you are defining those files that you want to scan. When you enable Exclude File Extensions, you are defining those files you do not want to scan.

.

For example:

By selecting *Exclude File Extensions*, Cheyenne Antivirus will scan all files except the following extensions.



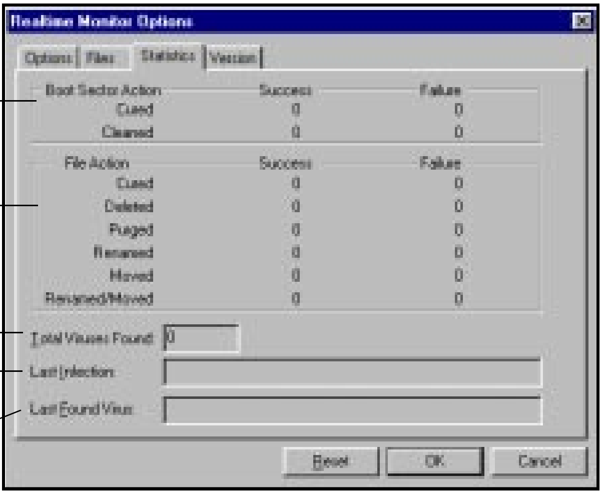
You can Add or Delete here to alter the list of file extensions to exclude from the scan.

4. From the Real-time Monitor Options, under Files tab, you can select Scan Compressed Files and add or delete Compressed File Extensions.

   To deselect scanning of your compressed files and their extensions, click off the checked box at the default setting of *Scan Compressed File*. We currently support PKZIP, ARJ, LHA, LZH, MIME, UUEncoded, and Microsoft compressed formats.

To view Statistics:

1. Choose the Statistics tab from the Real-time Monitor Options window. The following screen appears:



Boot Sector Action	Success	Failure
Cured	0	0
Cleaned	0	0

File Action	Success	Failure
Cured	0	0
Deleted	0	0
Purged	0	0
Renamed	0	0
Moved	0	0
Renamed/Moved	0	0

Total Viruses Found: 0

Last Infection:

Last Found Virus:

View the success/failure rates of the Cured and Cleaned files in the Boot Sector.

Listed here are the success/ failure rates for all File Actions.

The total number of viruses found.

Here is the last infected file name.

Here is the virus name for the last found virus.

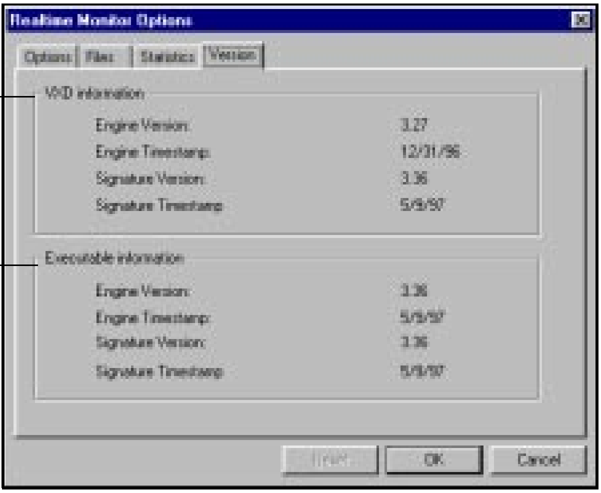
2. From the Statistics screen, you can monitor data relating to:
   - ➢ the Cure and Clean success/failure rates in the Boot Sector
   - ➢ the success/failure rates of all File Actions taken
   - ➢ the total viruses found
   - ➢ the file name of the last infected file
   - ➢ the virus name of the last found virus.

To verify the actions taken when a virus is detected:

1. Click on the Statistics tab from the Real-time Monitor Options screen to verify the success/failure rates of detected viruses and of these seven File Actions categories:
   - ➢ Cured
   - ➢ Deleted
   - ➢ Purged
   - ➢ Renamed
   - ➢ Moved
   - ➢ Renamed/Moved

To view signature file, VxD driver and REALMON.EXE Executable version information:

1. Click the Version tab from the Real-time Monitor Options. The following screen appears:



VxD information

Engine Version: 3.27
Engine Timestamp: 12/31/96
Signature Version: 3.36
Signature Timestamp: 5/9/97

Executable information

Engine Version: 3.36
Engine Timestamp: 5/9/97
Signature Version: 3.36
Signature Timestamp: 5/9/97

Virtual Device Driver Signature and Engine Version Information.

Executable Signature and Engine Version Information.

2. The Version tab shows you version information for the Real-time Monitor.

Password-Protection for the Real-time Monitor

The Real-time Monitor Options may be Password-Protected. Password Protection allows administrators the option to prevent users from changing and/or disabling the Real-time Monitor configurations.

Administrators can activate Password Protection after or prior to rolling out Cheyenne Antivirus for Windows 95 in their enterprise(s). Please see ‘About Password Protection’ for information on this procedure.

Suspend Time for Password-Protection

Suspend Time is an advanced feature which ships with Password-Protection that makes it possible for users to temporarily disable the Real-time Monitor for a configurable period of time. The intention of this feature is to allow users a window of opportunity to bypass the given Real-Time configurations to install software which otherwise could not be installed.

Using Rescue Disk to protect your critical disk areas

The critical disk areas of a workstation include the following:

- ➢ Master Boot Record
- ➢ Boot Sector
- ➢ Partition Table
- ➢ CMOS Settings
- ➢ I/O System file
- ➢ Windows 95 system file
- ➢ Windows 95 shell file (COMMAND.COM)

The Rescue Disk contains a backup of the critical disk areas. In addition, it is bootable and contains INOCUCMD.EXE. INOCUCMD is used to restore the backed up critical disk areas should your machine become infected and unbootable.

Through Cheyenne AntiVirus's Rescue Disk feature, you can make a backup of your critical disk area, examine the area for viruses and changes, and restore the area from a Rescue Disk backup diskette.

NOTE: We strongly recommend using Cheyenne AntiVirus to create a Rescue Disk. This extra precaution may be a life saver if a virus is encountered. After creating a Rescue Disk, label it clearly (making sure you note the specific workstation it belongs to) and store it in a safe place.

It is very important to maintain an up-to-date Rescue Disk for your workstation. This preventative measure should be performed on a scheduled basis.

Creating a Cheyenne AntiVirus Rescue Disk

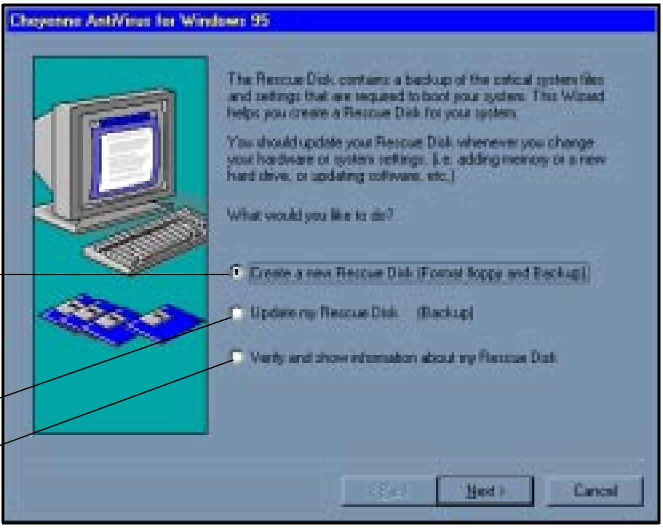
Back up Rescue Disk

You should create a Rescue Disk anytime you change your CMOS information, change your hardware, change your system files (such as by adding new lines to the AUTOEXEC.BAT when installing a product), or when you upgrade your operating system.

To create a new Rescue Disk

1. Click the Rescue Disk icon from the Toolbar or from the Quick Access menu.

   The Rescue Disk screen appears:



Cheyenne AntiVirus for Windows 95

The Rescue Disk contains a backup of the critical system files and settings that are required to boot your system. This Wizard helps you create a Rescue Disk for your system.

You should update your Rescue Disk whenever you change your hardware or system settings. (i.e. adding memory or a new hard drive, or updating software, etc.)

What would you like to do?

● Create a new Rescue Disk (Format floppy and Backup)

○ Update my Rescue Disk (Backup)

○ Verify and show information about my Rescue Disk

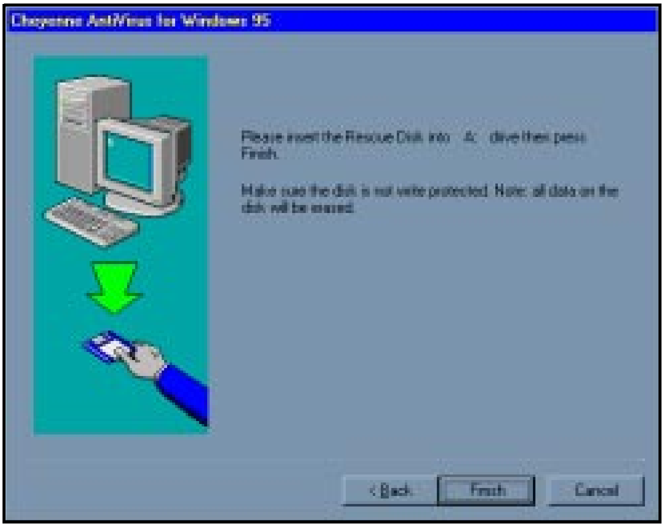
Click here on the Wizard to create a new Rescue Disk.

You should update your Rescue Disk whenever you change hardware or system settings.

Click here on the Wizard to verify information about the Rescue Disk.

2. To create a new Rescue Disk for your system, click on that option button from the Rescue Disk Wizard.

The following screen appears:



Please insert the Rescue Disk into A: drive then press Finish.

Make sure the disk is not write protected. Note: all data on the disk will be erased.

3. Insert your Rescue Disk diskette into the A: drive. Ensure that the disk is not write-protected.

   Click Finish to complete creating a new Rescue Disk.

4. Label the Rescue Disk and store it in a safe place.

   This Rescue Disk lets you start Windows 95 and Cheyenne Antivirus in the event of a serious disk infection. It is very important that the Rescue Disk be carefully labeled as belonging to a particular workstation.

To update and verify your Rescue Disk

To update your Rescue Disk:

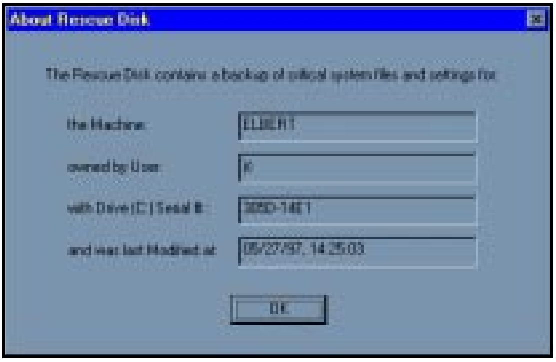
1. A quicker procedure to update your Rescue Disk is to click on the Update my Rescue Disk option from the Rescue Disk Wizard.

   Doing so is faster because it updates the disk without having to re-format it.

To verify your Rescue Disk:

1. To verify and display information about the Rescue Disk for your machine, click on that option button from the Wizard.

   The following screen appears:



About Rescue Disk

The Rescue Disk contains a backup of critical system files and settings for:

the Machine: ELBERT

owned by User: K

with Drive (C:) Serial #: 3050-14E1

and was last Modified at: 05/27/97, 14:25:03

Verify here the critical system files and settings contained on the Rescue Disk for this specific machine.

Click OK and Finish to complete verification of the Rescue Disk.

What's on your Rescue Disk

When you create a Rescue Disk, the following occurs:

- The disk is formatted and made bootable
- Cheyenne Antivirus files, INOCUCMD.EXE and VIRSIG.DAT, are copied
- HIMEM.SYS file is copied
- CONFIG.SYS file is created with the following two lines:

```
FILES=40

DEVICE=HIMEM.SYS
```

- AUTOEXEC.BAT is created to invoke INOCUCMD.EXE
- Rescue Disk is volume-labeled
- The following critical disk area information is backed up:

Critical Disk Area Information	File
CMOS settings	CMOS.SIG
Partition table	PARTSECT.SIG
Boot sector	BOOTSECT.SIG
Windows 95 system file	DOS.SIG
Windows 95 shell file (COMMAND.COM)	SHELL.SIG
BIOS system file	BIOS.SIG
CONFIG.SYS file	CONFIG.SIG
AUTOEXEC.BAT file	AUTOEXEC.SIG
Information about the above files and their location on the hard disk	INFO.SIG

What to do if Cheyenne AntiVirus discovers a virus

Required items

In order to recover from a virus you need the following:

- ➢ A write-protected copy of the Cheyenne AntiVirus for Windows 95 installation diskettes.
- ➢ An up-to-date Rescue Disk containing the latest backup of your critical disk areas.

It is very important to maintain an up-to-date Rescue Disk backup for each workstation. The Rescue Disk backup is created by using the Rescue Disk option.

NOTE:If you have not yet created your Rescue Disk and are not currently experiencing a virus attack, we highly recommend that you create a Rescue Disk now. Please label your Rescue Disk and place it in a secure place.

Infected file detected or an infection found in memory

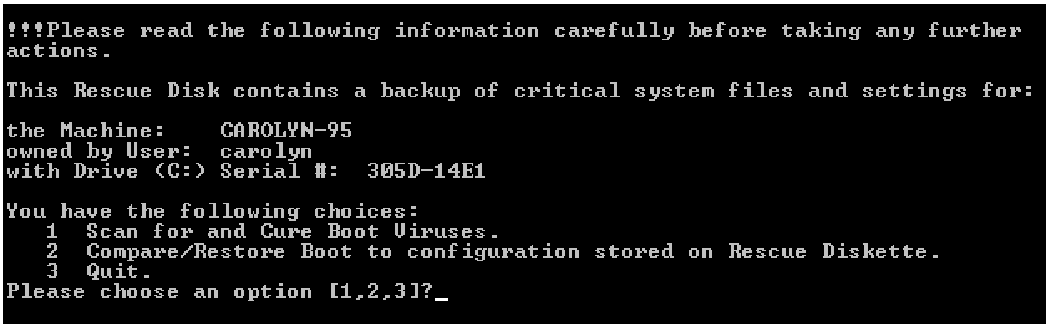
You should do the following if an infected file is detected or an infection is found in memory:

1. Cold boot the computer (power off) with the Rescue Disk inserted.

   See section *Create an Cheyenne AntiVirus Rescue Disk diskette.*

2. After booting, you are presented with a DOS screen showing information pertaining to this Rescue Disk.

You will see a DOS screen similar to this sample:



```
!!!Please read the following information carefully before taking any further
actions.

This Rescue Disk contains a backup of critical system files and settings for:

the Machine:    CAROLYN-95
owned by User:  carolyn
with Drive (C:) Serial #:  305D-14E1

You have the following choices:
   1  Scan for and Cure Boot Viruses.
   2  Compare/Restore Boot to configuration stored on Rescue Diskette.
   3  Quit.
Please choose an option [1,2,3]?_
```

Please verify that this is the correct Rescue Disk.

3. Please select option 1 to Scan for and Cure Boot Viruses.

4. At this point, your machine searches for memory and boot sector viruses.

5. Go to the Inoculan directory on your hard drive and run INOCUCMD.EXE to scan your hard drive for possible viruses.

   For information about the INOCUCMD.EXE syntax, see section *Using the DOS command line scanner.*

6. Delete any infected files identified (or scan again with the Delete File option turned on) and replace the files from a reliable source.

   As a last resort option, you can scan with the *Cure File* option selected.

7. Re-scan the hard disk after replacing infected files to ensure the virus has been removed from the system.

8. Reboot your machine to return to Windows 95.

Boot sector virus detected or suspected

You should do the following if a boot sector virus is detected or suspected:

1. Cold boot the computer (power off) with the Rescue Disk inserted.

   See section *Create an Cheyenne AntiVirus Rescue Disk diskette.*

2. After booting, you are presented with a screen showing information pertaining to this Rescue Disk. Please verify that this is the correct Rescue Disk.

3. Please select option 1 to Scan for and Cure Boot Viruses.

4. At this point, your machine searches for memory and boot sector viruses.

5. If all is well, remove the Rescue Disk and reboot your machine.

Cannot boot machine

Depending on the degree of damage, a virus can alter all or derail the critical disk areas on your machine. This may render your machine unbootable, or your machine may not function properly.

To restore the critical disk areas of your machine:

1. Cold boot the computer (power off) with the Rescue Disk inserted.

   See section *Create an Cheyenne AntiVirus Rescue Disk diskette.*

2. After booting, you are presented with a screen showing information pertaining to this Rescue Disk. Please verify that this is the correct Rescue Disk.

3. Please select option 2 to restore the critical disk areas of your machine.

4. At this point, your machine searches for memory and boot sector viruses.

5. If all is well, remove the Rescue Disk and reboot your machine.

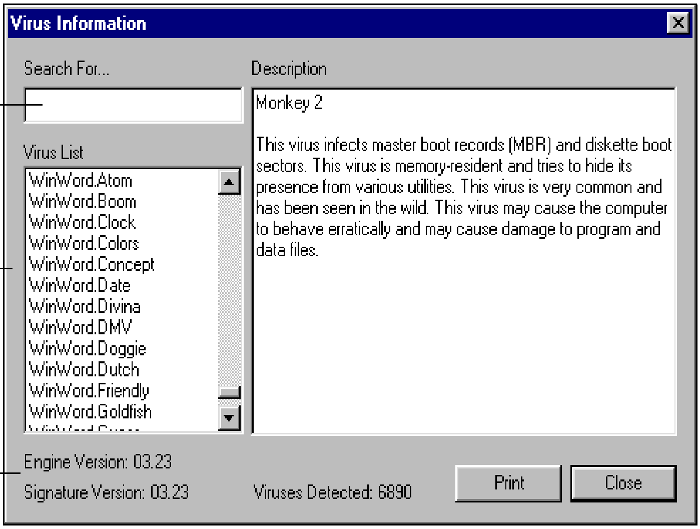
Keeping your AntiVirus system up-to-date

Part of the process of safeguarding your workstation against viruses involves keeping your Cheyenne AntiVirus system up-to-date with the latest software available. This section will discuss how you can get the latest virus detection engines and the monthly virus signature files.

NOTE:New viruses are being written every day. You should keep your Cheyenne AntiVirus virus signature files and virus engines current. Thus you prevent infection from the latest viruses.

How to Check the Version of the Virus Signature and Engine

After launching the Cheyenne AntiVirus for Windows 95 program, you can click on Help from the menu bar and select About Virus Signature. This help menu displays the virus signature file version, and also some virus descriptions. It also provide the virus engine version.



Search For...

Virus List

WinWord.Atom
WinWord.Boom
WinWord.Clock
WinWord.Colors
WinWord.Concept
WinWord.Date
WinWord.Divina
WinWord.DMV
WinWord.Doggie
WinWord.Dutch
WinWord.Friendly
WinWord.Goldfish

Description

Monkey 2

This virus infects master boot records (MBR) and diskette boot sectors. This virus is memory-resident and tries to hide its presence from various utilities. This virus is very common and has been seen in the wild. This virus may cause the computer to behave erratically and may cause damage to program and data files.

Engine Version: 03.23
Signature Version: 03.23
Viruses Detected: 6890

You can search for a specific virus here.

A listing of all viruses that the engine will detect.

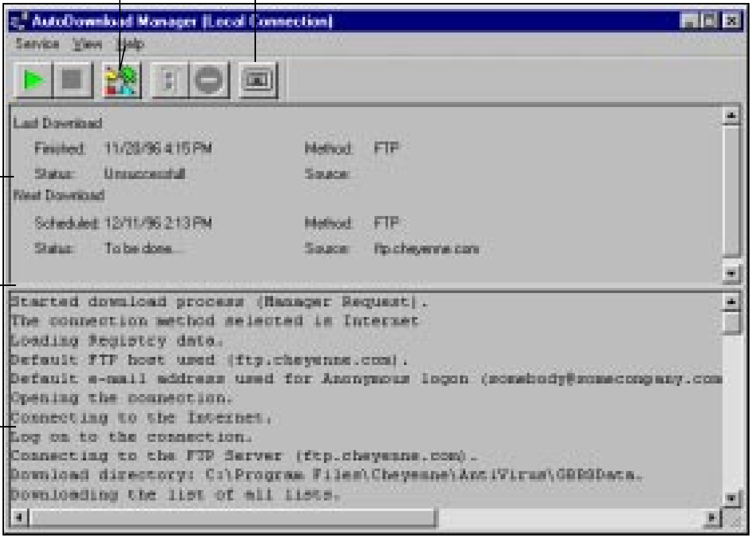
This is where the virus signature and detection engine version is displayed.

How to use the AutoDownload Manager

The Cheyenne AutoDownload Manager is an online utility program that can be run separately to download the latest signature files and virus engines. Once configured, the program can help you keep the Windows 95 system fully updated automatically.

To launch the Cheyenne AutoDownload Manager, you can click on the Start button on the task manager bar, then select Programs, Cheyenne AntiVirus for Windows 95, and then AutoDownload Manger.

Once the AutoDownload Manager launches, this screen appears:



Last Download

Finished: 11/28/96 4:15 PM   Method: FTP
Status: Unsuccessful   Source:

Next Download

Scheduled: 12/11/96 2:13 PM   Method: FTP
Status: To be done...   Source: ftp.cheyenne.com

```
Started download process (Manager Request).
The connection method selected is Internet
Loading Registry data.
Default FTP host used (ftp.cheyenne.com).
Default e-mail address used for Anonymous logon (somebody@somecompany.com
Opening the connection.
Connecting to the Internet.
Log on to the connection.
Connecting to the FTP Server (ftp.cheyenne.com).
Download directory: C:\Program Files\Cheyenne\AntiVirus\GBBSData.
Downloading the list of all lists.
```

This is the configuration or properties button. You can use this button to set the properties of your connection type.

This button clears the terminal screen.

This is your connection window.

This bar can be adjusted to customize the window size.

This is your connected session window.

How to start the AutoDownload Manager:

1. Before any files can be downloaded, the AutoDownload Agent must be running. By default, the Agent will be running when you open the AutoDownload manager screen. If the Agent is running, the Start button (shown at left) will be grey. If the Agent is not running, the Start button will be green.

2. If the AutoDownload Agent is running, you can click on the Start Download Session button to begin downloading the latest updates. The AutoDownload manager downloads the latest files automatically. The program knows exactly which directories and files to download.

How to stop the AutoDownload Manager:

1. To halt the download session, just click on the Abort Download Session button. This button stops the transfer of files from the Cheyenne download sites.

2. To stop the AutoDownload Agent, just click on the Stop the AutoDownload Agent button. This button stops the AutoDownload Agent. The Agent has to be running for any downloads to take place.

How to clear the terminal screen:

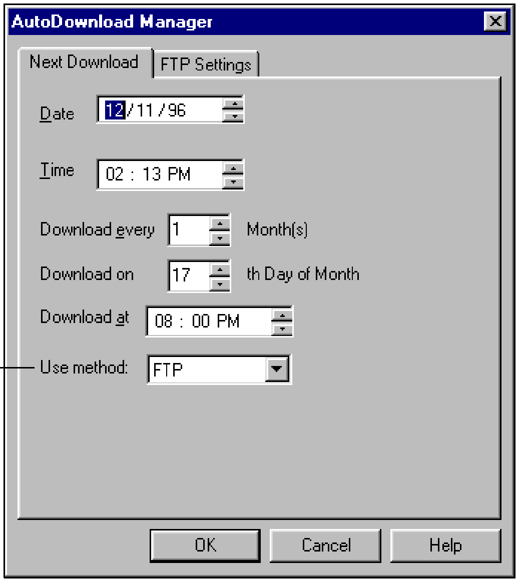
1. To clear the terminal screen after transferring files from the Cheyenne download sites, just click on the Clear the terminal screen button from the AutoDownload Manager.

Configuring the AutoDownload Manager

To configure the AutoDownload Manager,

1. Click on the Configuration button, or choose Properties from View on the menu bar.

   The following screen appears:



Date 12/11/96

Time 02 : 13 PM

Download every 1 Month(s)

Download on 17 th Day of Month

Download at 08 : 00 PM

Use method: FTP

You can schedule the update time, date and/or frequency here.

This toggles between modem or ftp connection types.

NOTE:If you are dialing into the Cheyenne BBS through a modem, you must attach the modem to the workstation.

There are two different methods of downloading.

- You can use the internet ftp protocol to connect to the Cheyenne Software site.
- You can connect to Cheyenne Software through a dialup asynchronous modem. Once the *Modem (BBS)* has been

selected, you can enter in the appropriate values in the fields provided. The default settings should be tried first.

If you are already connected to a network that has internet connectivity, the AutoDownload manager will connect, download, and update the AntiVirus program automatically. If you are using a dialup internet service provider, Windows 95 will automatically sense the AutoDownload manager program and begin the dialup connection to your internet service provider. The AutoDownload manager will then begin login on to the ftp.cheyenne.com site.

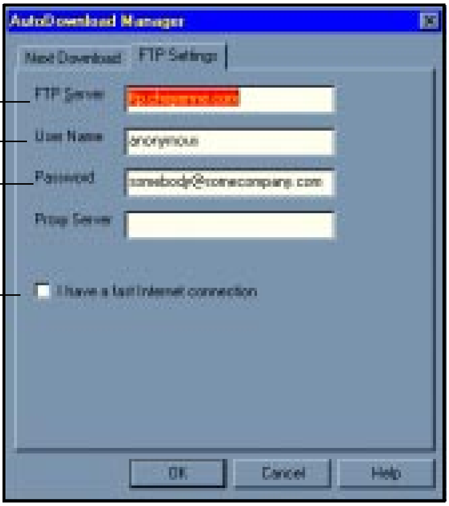
NOTE:The AutoDownload manager is already configured to the correct ftp login and connection information. Try connecting to our site using the default values first.

Configuring FTP Settings

To configure the FTP settings:

1. Select FTP from the “Use Method” drop-down box.

2. Click on the FTP Settings tab:



FTP Server: [illegible]

User Name: anonymous

Password: somebody@somecompany.com

Proxy Server:

□ I have a fast Internet connection

This field shows the Cheyenne ftp address.

This field displays the login user name.

This field displays the ftp login password.

You can select this box if you have a high speed connection to the internet.

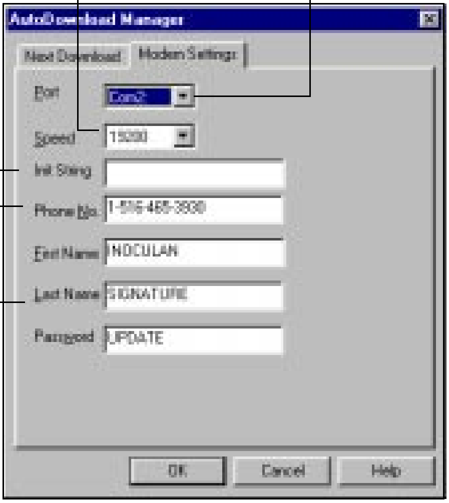
3. Click OK for your settings to take effect.

Configuring Modem Settings

To configure the modem settings:

1. Select “Modem (BBS)” from the “Use Method” drop-down box.

2. Click the Modem Settings tab and make your selections as needed.



Port: Com2

Speed: 19200

Init String:

Phone No.: 1-516-465-3930

First Name: INOCULAN

Last Name: SIGNATURE

Password: UPDATE

This field allows you to toggle the speed of your modem connection.

This field allows you to choose the correct port to which your modem is

This field allows you to enter a specific AT modem command string if your modem requires specific initializing commands.

This is the Cheyenne BBS phone number.

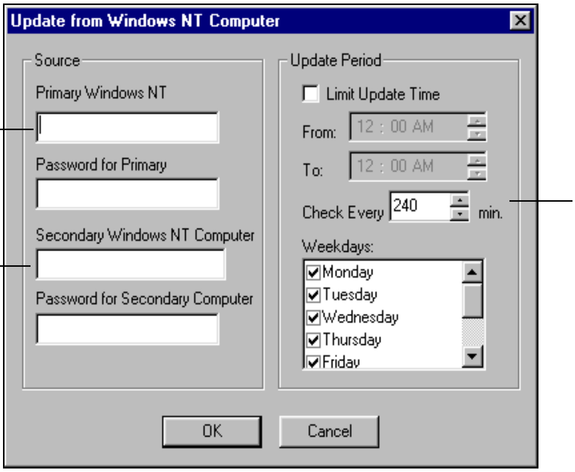
This field is the sign-on procedure for the Cheyenne BBS protocols. The default values are the correct information.

3. Click OK for your settings to take effect.

Scheduled Updates from Windows NT

You can schedule regular virus signature file updates from a Windows NT computer. To do so, just select the Scheduled Scan menu from the Quick Access menu. Select the *Load Signature Update from a Windows NT Computer* button.

This configuration screen appears:



Primary Windows NT:

Password for Primary:

Secondary Windows NT Computer:

Password for Secondary Computer:

□ Limit Update Time

From: 12 : 00 AM

To: 12 : 00 AM

Check Every 240 min.

Weekdays:
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday

Enter the default Windows NT computer login name and password. The Windows NT machine must have InocuLAN installed.

Enter a secondary Windows NT machine with InocuLAN installed here.

Configure the time interval of the virus signature updates here.

NOTE:The Windows NT machines must have InocuLAN anti-virus software installed. The update will search through the directory structure of the Windows NT to find the latest version of the virus signature, and detection engines.

Troubleshooting the connection

If you are experiencing problems with modem connectivity, you should try:

- ➢ Connecting at a lower modem speed

- ➢ Check the phone line to make sure the line is active
- ➢ Make sure the modem is connected and seated properly to the computer (the cables, the ports, and the power supply)

NOTE:The AutoDownload manager is already configured to the correct modem sign-on information to connect to the Cheyenne BBS. Try connecting to our site using the default values first.

Where do Cheyenne AntiVirus updates come from?

Cheyenne AntiVirus update are available on-line through Cheyenne's bulletin board, through CompuServe, through ftp downloads, or our world wide web site. The monthly updates contain the latest virus signature files, and/or other necessary component files.

Getting updates from the bulletin board

Cheyenne Software has public Cheyenne AntiVirus directories on its bulletin board (BBS), CompuServe, internet FTP/Web Pages worldwide. So get on-line to download the latest virus signature files!

8

Chapter

USING ANTIVIRUS FOR WINDOWS

To keep your network virus-free, you must keep the viruses from gaining access to your network.

In this chapter, you will learn:

Page	
8-3 ➢	How to Install AntiVirus for Windows 3.1x
8-17 ➢	How to Use Quick Access
8-20 ➢	How to Use the Local Scanner
8-37 ➢	How to Keep your Workstation Virus-Free
8-39 ➢	About the WIMMUNE real-time Monitor

8-41 ➢ How to Protect your Critical Disk Area

8-46 ➢ How to Use the EXAMINE utility

Installing Cheyenne AntiVirus for Windows

Before you install Cheyenne AntiVirus for Windows or DOS, make sure that you:

- Evaluate Cheyenne AntiVirus hardware and software requirements.
- Configure your system files: CONFIG.SYS and AUTOEXEC.BAT.
- Scan your system for viruses using the Cheyenne AntiVirus for DOS.

System requirements

To install and use Cheyenne AntiVirus on your workstation, the following hardware and software requirements must be satisfied:

	Workstation
Machine Type/ Memory	IBM PC, AT, PS/2 or compatible with 4 MB RAM (8 MB RAM recommended for Cheyenne AntiVirus for Windows) For Cheyenne AntiVirus for DOS Manager, 470K conventional memory. 1M extended memory is recommended.
Disk Space	6 MB of disk space for Windows manager 2 MB of disk space for DOS manager
Software	-DOS 3.x and above CONFIG.SYS must be set to a minimum of: FILES=40 -Windows 3.1 or higher for Windows Manager

Configuring your system for installation

Configure your system files before installing Cheyenne AntiVirus, to ensure proper installation and use of this product.

To configure your system files:

1. Turn off the power to your workstation.

2. Boot your workstation with a write-protected, virus-free boot diskette (such as the original operating system diskette).

   The CONFIG.SYS on this diskette must have FILES=40 or a higher number. It is recommended that you also add the statement DEVICE=HIMEM.SYS. For this statement to work, you must copy the HIMEM.SYS file, located in the DOS directory, on to the diskette.

   If you do not have a CONFIG.SYS on your diskette, you can add the necessary information using the following procedure. *Since your own workstation may have already been infected, it is highly recommended that you do the following at another workstation which is infection free.* If no other workstation is available, perform the following AFTER booting your workstation with the boot diskette:

   - At the A prompt, type:

     ```
     COPY CONFIG.SYS   <ENTER>
     ```

   - With the cursor flashing, type:

     ```
     FILES=40
     DEVICE=HIMEM.SYS <F6>  <ENTER>
     ```

Note that you must disable write-protection to create the CONFIG.SYS file. After creating it, re-enable write-protection on the diskette.

3. Re-boot your workstation.

Windows Installation

To install Cheyenne AntiVirus for Windows:

1. Insert the Cheyenne AntiVirus Installation CD-ROM into the drive.

2. Choose Run from the File Menu in the Windows Program Manager.

   The Run dialog box opens.

3. In the text box, type `D:SETUP` (if `D` is the drive containing the installation disk) and then click OK.

   The Cheyenne AntiVirus setup program begins.

4. Enter your name and company.

5. Note the system requirements for Cheyenne AntiVirus. Select Continue when done.

6. Choose one of the following Setup options:

   - *Express Setup:* to install both the DOS and Windows managers. This option also adds statements to your AUTOEXEC.BAT to run IMMUNE and EXAMINE, and sets the path for Cheyenne AntiVirus home directory. IMMUNE is a TSR that scans files on your workstation for viruses each time a file is executed, accessed, or opened. EXAMINE is a program that checks your workstation for changes to the Critical Disk Area.
   - *Custom Setup:* to select the manager you want to install. This option also lets you select the options you want to add to your AUTOEXEC.BAT.

Instructions for each Setup option can be found in the next two sections of this chapter. Please refer to the appropriate section for the option you are using.

Express Setup

If you have selected the Express Setup option:

1. Specify an installation directory and click Continue.

   The Setup program copies the Cheyenne AntiVirus files to your system.

   Your AUTOEXEC.BAT is modified to load IMMUNE and EXAMINE. A statement that sets the path of Cheyenne AntiVirus home directory is also added. The original file is saved in Cheyenne AntiVirus home directory as AUTOEXEC.BAK.

   Your system's Critical Disk Area is backed up to the destination directory. This is done so that recovery from a viral infection or other corruption of this disk area can be accomplished, if necessary.

2. Specify if you want to create a rescue diskette.

   A rescue diskette is a backup of the Critical Disk Area.

NOTE: While you can back up your Critical Disk Area once Cheyenne AntiVirus is loaded on your workstation, we strongly recommend that you take the time to perform this step now. This extra precaution may be a life saver if a virus is encountered.

The diskette you use should be a DOS system diskette with a CONFIG.SYS file that has FILES=40 or a higher number. Write-protection should be added after the rescue diskette is created.

Warning: The backup diskette should be clearly labeled as belonging to a particular workstation, and stored in a safe place. Because the backup contains information specific to a workstation, *using a backup diskette from a different workstation may cause severe problems*.

Once the rescue diskette is created, the installation of the Cheyenne AntiVirus Manager is complete. You will see a message that says Cheyenne AntiVirus was installed successfully.

Custom Setup

If you have selected the Custom Setup option:

1. Select one or both of the following Managers to install:
   - Windows Manager
   - DOS Manager

2. Specify an installation directory and click Continue.

   The Setup program copies the Cheyenne AntiVirus files to your system.

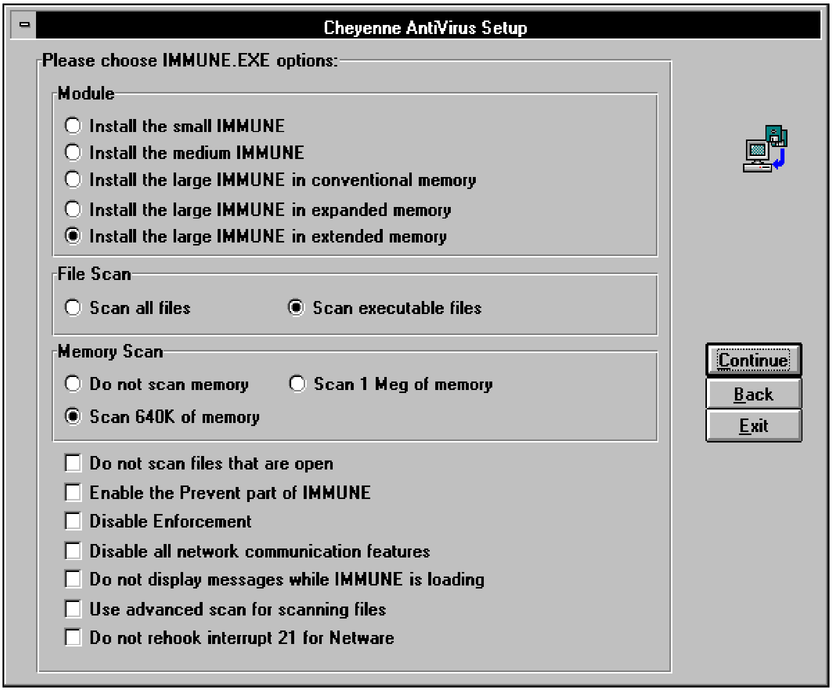
3. Select the options you would like added to your AUTOEXEC.BAT file.

The available options are briefly explained below. Details on these options are provided later in this chapter.

Option	Change to AUTOEXEC.BAT
Set Environment Variable	Modifies your PATH statement to include the Cheyenne AntiVirus directory. For example, if you chose the install to the Cheyenne AntiVirus directory on your C drive, the added statement will be: SET ANTIVIRUS=C:\ANTIVIRUS
EXAMINE.EXE	Adds the EXAMINE program. EXAMINE checks your workstation for changes to the Critical Disk Area.
IMMUNE.EXE	Adds the IMMUNE program. IMMUNE scans files on your workstation in real-time every time a file is executed, accessed or opened. IMMUNE is a DOS TSR that runs only in a DOS environment. If you are using Windows, real-time scanning is done by the WIMMUNE program. Selecting this option also install the WIMMUNE program.

4. If you chose the Set Environment Variable option, you will see a message telling you the AUTOEXEC.BAT file has been updated.

5. If you chose the IMMUNE.EXE option, you can accept the default settings or select other options, as shown below:



Cheyenne AntiVirus Setup

Please choose IMMUNE.EXE options:

Module

○ Install the small IMMUNE
○ Install the medium IMMUNE
○ Install the large IMMUNE in conventional memory
○ Install the large IMMUNE in expanded memory
● Install the large IMMUNE in extended memory

File Scan

○ Scan all files ● Scan executable files

Memory Scan

○ Do not scan memory ○ Scan 1 Meg of memory
● Scan 640K of memory

☐ Do not scan files that are open
☐ Enable the Prevent part of IMMUNE
☐ Disable Enforcement
☐ Disable all network communication features
☐ Do not display messages while IMMUNE is loading
☐ Use advanced scan for scanning files
☐ Do not rehook interrupt 21 for Netware

Select the options you prefer. The IMMUNE options are described in the following tables:

Module Options	Description
Install the small IMMUNE	Loads the small version of IMMUNE. About 11-13 K of conventional memory will be used.
Install the medium IMMUNE	Installs the medium version of IMMUNE. About 30 K of conventional memory will be used.
Install the large IMMUNE in conventional memory	Installs the large version of IMMUNE in conventional memory. About 109 K of conventional memory will be used.

Module Options	Description
Install the large IMMUNE in expanded memory	Installs the large version of IMMUNE in expanded memory. About 7K of conventional memory will also be used.
Install the large IMMUNE in extended memory	Installs the large version of IMMUNE in extended memory. About 7K of conventional memory will also be used.

File Scan Options	Description
Scan all files	Scans all files (not just executable files). This option requires a large amount of CPU resources.
Scan executable files	Scans only executable files. This is the default.

Memory Scan Options	Description
Do not scan memory	Does not scan memory.
Scan 1 Meg of memory	Scans 1 Meg of memory.
Scan 640K of memory	Scans 640 K of memory. This is the default value.

Other Options	Description
Do not scan files that are open	Does not scan files that are open.
Enable the Prevent part of IMMUNE	Monitors your workstation for virus-like behavior, such as unauthorized formatting of your hard disk.

Other Options	Description
Disable Enforcement	Removes Enforcement for your workstation. Use if your workstation does not log in to an Cheyenne AntiVirus domain server. For memory management purposes, this option removes the Enforcement capability from IMMUNE. This option is solely for stand-alone environments.
Disable all network communication features	Disables all network communication features. Use for stand-alone workstations. This option reduces the size of the small version of IMMUNE.
Do not display messages while IMMUNE is loading	Does not display messages while IMMUNE is loading.
Use advanced scan for scanning files	Completely scans data files. Without this option, IMMUNE only checks the beginning and end of data files. Other types of files (*.EXE, *.COM, etc.) are always fully scanned. This option requires a large amount of CPU resources.
Do not rehook interrupt 21 for NetWare	Does not rehook interrupt 21 for DOS. Use if you have other TSRs that consistently rehook to this interrupt.

When you press Continue, your AUTOEXEC.BAT is modified according to your selections. The original file is saved as AUTOEXEC.BAK in Cheyenne AntiVirus home directory.

If you chose not to modify your AUTOEXEC.BAT, an AUTOEXEC.INO file is created in Cheyenne AntiVirus home directory. This file is a copy of your current AUTOEXEC.BAT with the recommended modifications that should be made. You can examine this file after the installation, and if you want, you can substitute this file for the AUTOEXEC.BAT you are currently using or you can add these statements to your current AUTOEXEC.BAT.

The AUTOEXEC.INO contains the following additional statements:

```
SET ANTIVIRUS=C:\ANTIVIRUS
C:\ANTIVIRUS\EXAMINE.EXE
C:\ANTIVIRUS\IMMUNE.EXE
```

Afterwards, the Critical Disk Area is backed up to the destination directory. This is done so that recovery from a viral infection or other corruption of this disk area can be accomplished, if necessary.

6. Specify if you want to create a rescue diskette.

   A rescue diskette is a backup of the Critical Disk Area.

NOTE: While you can back up your Critical Disk Area once Cheyenne AntiVirus is loaded on your workstation, <u>we strongly recommend that you take the time to perform this step now. This extra precaution may be a life saver if a virus is encountered</u>.

The diskette you use should be a DOS system diskette with a CONFIG.SYS file that has FILES=40 or a higher number. Write-protection should be added after the rescue diskette is created.

Warning: The backup diskette should be clearly labeled as belonging to a particular workstation, and stored in a safe place. Because the backup contains information specific to a workstation, *using a backup diskette from a different workstation may cause severe problems*.

Once the rescue diskette is created, the installation of the Cheyenne AntiVirus Manager is complete.

You will see a message that says Cheyenne AntiVirus was installed successfully.

Starting Cheyenne AntiVirus

This section explains how to start the Cheyenne AntiVirus for Windows Manager and Cheyenne AntiVirus for DOS Manager.

The Cheyenne AntiVirus for Windows Manager

Running Cheyenne AntiVirus for Windows on your workstation

You start the Cheyenne AntiVirus for Windows Manager the same way you start other Windows applications from the Program Manager.

To load Cheyenne AntiVirus for Windows:

1. Open the Cheyenne AntiVirus program group.

2. Double-click the Cheyenne AntiVirus for Windows icon.

   The Cheyenne AntiVirus program begins by checking itself and the workstation's memory. If there are no viruses detected in RAM, Cheyenne AntiVirus for Windows is displayed.

   If Cheyenne AntiVirus detects a virus loaded in memory, Cheyenne AntiVirus removes the virus and displays a message showing the number of viruses that were neutralized. Then, Cheyenne AntiVirus for Windows appears.

NOTE: Even though Cheyenne AntiVirus has removed the virus(es) from memory, you should reboot your workstation with a write-protected, clean boot diskette (such as the original operating system diskette) before continuing with Cheyenne AntiVirus.

The Cheyenne AntiVirus for DOS Manager

Running Cheyenne AntiVirus for DOS on your workstation

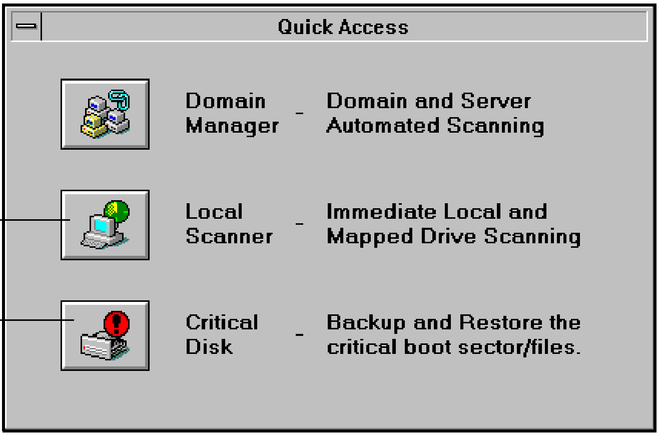
To load Cheyenne AntiVirus for DOS on a workstation:

1. Open the Cheyenne AntiVirus program group.

2. Double-click the Cheyenne AntiVirus for DOS Manager icon.

Using the Quick Access dialog box/toolbar

Cheyenne AntiVirus for Windows has a Quick Access box that allows you to select functions. It is accessed by double-clicking the Cheyenne AntiVirus for Windows icon.



Quick Access

Domain Manager - Domain and Server Automated Scanning

Local Scanner - Immediate Local and Mapped Drive Scanning

Critical Disk - Backup and Restore the critical boot sector/files.

Select to scan workstations or to view scanning records, the virus list, or version information.

Select to back up, restore, or examine your Critical Disk Area.

You can also use a toolbar by selecting the *View/Toolbar* option on Cheyenne AntiVirus menu bar.

Selecting a function

To select a function:

1. Click the button for the function you want.

Cheyenne AntiVirus virus list

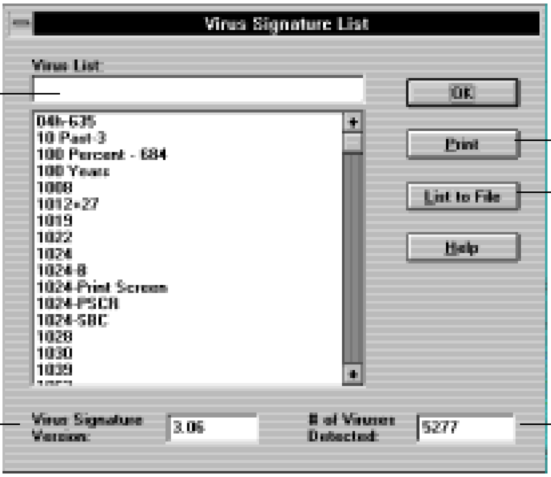
You can display or print a list of the viruses that Cheyenne AntiVirus can detect.

Displaying the virus list

To display the list:

1. Choose About Virus Signatures... from the Help menu.

   The list is displayed:



04h-635
10 Past-3
100 Percent - 684
100 Years
1008
1012+27
1019
1022
1024
1024-B
1024-Print Screen
1024-PSCR
1024-SBC
1028
1030
1039

Virus Signature Version: 3.06

# of Viruses Detected: 5277

Type the name of the virus you want to find.

This is a section of the list of viruses that Cheyenne AntiVirus can detect.

This is the version of the virus file on your workstation.

Click to print this list.

Click to create a report file.

This shows the number of viruses in the signature file.

Printing the virus list

To print a report:

1. Click the Print button.

Creating a report file

To create a report file:

1. Click the List to File button.
2. Enter a path and file name for the report.

The report is an unformatted text file (ASCII) which can be formatted and printed using a suitable word processor or text editor.

Using the Local Scanner

The Local Scanner scans files on a local workstation or a server.   The server to be scanned does not have to be an InocuLAN server, but you must be connected to the server. The actual scanning is done by the InocuLAN for Windows Manager on the local workstation.

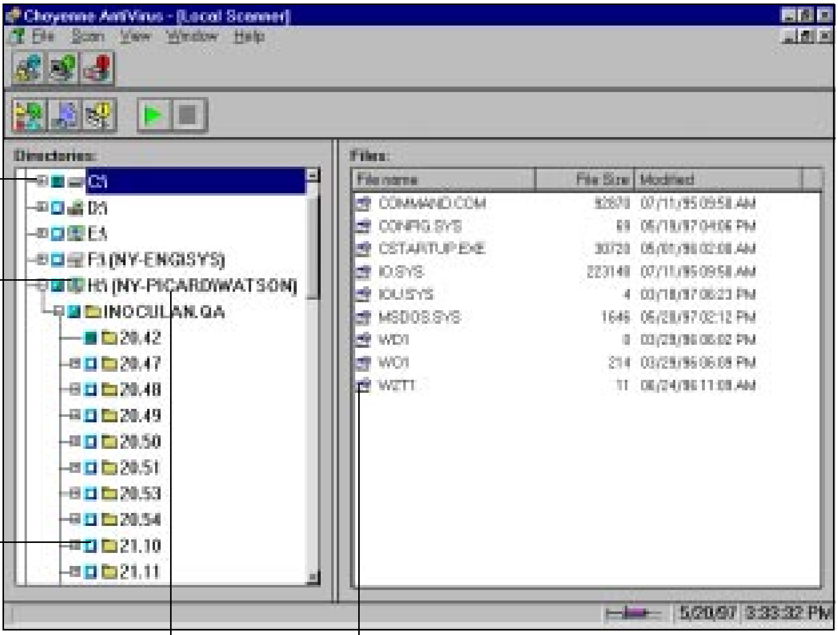
NOTE:You cannot use the Local Scanner on a server that has real-time scanning enabled with the outgoing files option selected. Viruses will be reported by the Real-time Monitor. Instead, you can use the Domain Manager for these servers.

Instructions for a basic scan

Follow the instructions below to perform a basic scan (without any options or filters) using the Local Scanner. Information about using options and filters begins in the next section.

1. Click the Local Scanner button.

InocuLAN reads all of the directories on the drive where InocuLAN's home directory is located before the Local Scanner screen appears:



```
C:\
D:\
E:\
F:\ [NY-ENGSYS]
H:\ [NY-PICARD\WATSON]
  INOCULAN.QA
    20.42
    20.47
    20.48
    20.49
    20.50
    20.51
    20.53
    20.54
    21.10
    21.11
```

File name	File Size	Modified
COMMAND.COM	92870	07/11/95 09:58 AM
CONFIG.SYS	69	05/19/97 04:06 PM
CSTARTUP.EXE	30720	05/01/96 02:08 AM
IO.SYS	223148	07/11/95 09:58 AM
IOU.SYS	4	03/18/97 06:23 PM
MSDOS.SYS	1646	05/28/97 02:12 PM
WD1	0	03/29/96 06:02 PM
WO1	214	03/29/96 06:08 PM
WZT1	11	06/24/96 11:08 AM

5/20/97 3:33:32 PM

Half shaded target boxes indicates a partial volume scan selection.

If a volume is displayed with a green border and the letter R in blue, the volume is protected by the Server Real-time Monitor program.

Click the light blue selection boxes to green to choose a drive or mapped volume to scan for viruses.

Displays volume information.

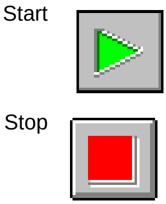
A file with a magnifying glass indicates a targeted file for a scan job.

2. Select what to scan.

   The entire drive is automatically selected for you. You can scan this drive or you can select another.

   If you want to scan the entire drive, but you want to exclude a specific directory, double-click on that directory.

   If you only want to scan specific files or directories, double-click the drive letter (to de-select everything) and then double-click on each file or directory you want to scan. If you are selecting specific files, the files must ALL be in the same directory.



3. Click the Start button.

   The scan begins immediately.

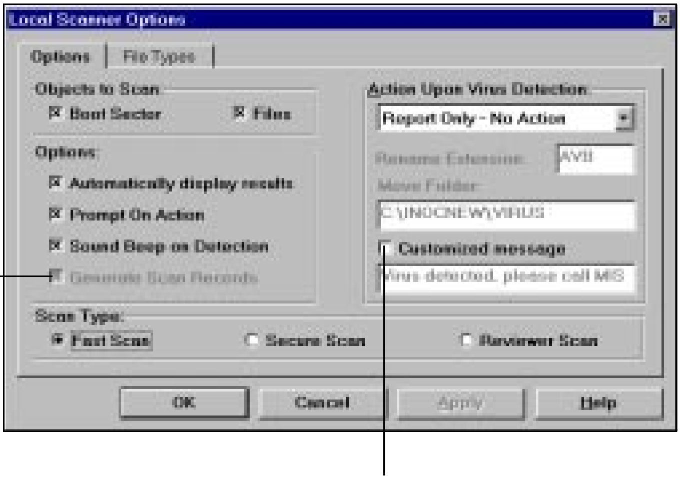
   After the scan begins, the Start button turns gray, and the Stop button turns red. Click the Stop button at any point to stop the scanning process.

Options for Workstation Scans

To apply an option:

1. Click the Configuration button on the Local Scanner screen.

   The Local Scanner Options screen appears:



Local Scanner Options

Options | File Types

Objects to Scan
☒ Boot Sector ☒ Files

Options
☒ Automatically display results
☒ Prompt On Action
☒ Sound Beep on Detection
☒ Generate Scan Records

Action Upon Virus Detection
Report Only - No Action
Rename Extension: AVB
Move Folder: C:\INOCNEW\VIRUS
□ Customized message
Virus detected, please call MIS

Scan Type:
● Fast Scan ○ Secure Scan ○ Reviewer Scan

Check this box to enable or disable the Scan Records option.

Check this box the enable Customized message option to be displayed upon virus detection. Type in the field provided to display your personal message.

2. Select the options you want to include with the scanning job.

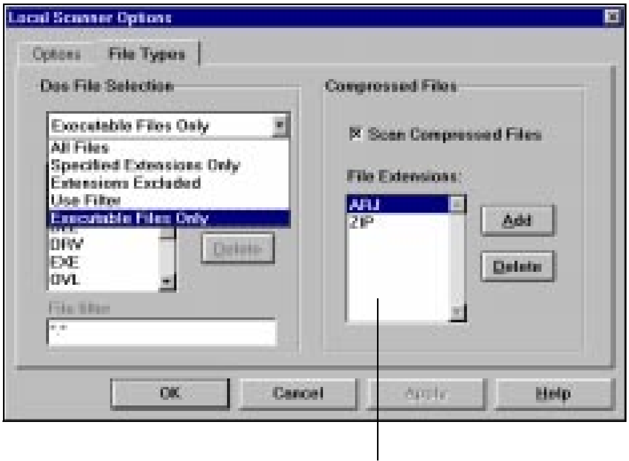
Objects to Scan

You can select to scan the boot sector (which contains code that is executed when the system is booted) and/or files.

NOTE:Some options like the Splash Screen disable box, the Mapped Drive information box, or the Change Configuration enable box on the Cheyenne AntiVirus Scanner program are not enabled until the InocuLAN servers and workstations are updated with the AVUPDATE program. For further information on these options, please refer to your AVUPDATE manual.

File Selection

Select the File Types tab on the Local Scanner Option menu to choose from 5 different file types to be filtered or scanned. This menu will appear:



You can also add various file compression types to be included in the scan job.

You can select *All Files*, *Specific Extension Only*, *Extension*s *Excluded*, *Use Filter*, or a selection of *Executable Files Only*. If you select *Specified Extensions Only* option, you can further define which files to scan by their extensions. If you select the *Use Filter* option, you can insert astericks (*) in the File Filter field to represent a wildcard filter.

Action Upon Virus Detection

Select one of the options described below. (Regardless of which option you choose, a message will be broadcast when a virus is detected.)

Action	Description
Report Only - No Action	Displays an on-screen report that lists the infected files and the virus that was detected. This information also appears in the Scanning Report.
Delete File	Deletes an infected file from a workstation.
Cure File	Removes certain known viruses from infected files and restores the files to their original state. If the file cannot be cured, it will be renamed with an .AVB extension (refer to ‘Rename File’ below). Even if InocuLAN cures the file, we recommend you purge the infected file and then restore the original file.
Move File	Moves an infected file from its current directory to the INOCULAN\VIRUS directory.
Purge File	Deletes an infected file so that it cannot be recovered.
Rename File	Renames infected files by giving them an .AVB extension. Files with this extension will not be scanned by any of InocuLAN’s scanners (except the Real-time Monitor). If a file exists with the .AVB extension and an infected file in the same directory will result in the same file name, the .AVB extension will be changed. The extension will become .AV# and the number will be incremented for each subsequent occurrence (.AV0, .AV1, etc.). For example, an infected MOUSE.COM is renamed MOUSE.AVB and then an infected MOUSE.SYS is renamed to MOUSE.AV0.
Copy and Cure File	Will make a copy of the infected file to the INOCULAN\VIRUS directory and continues to cure the file.

Action	Description
Rename and Move File	Renames infected files by giving them a different extension and then moves them to the INOCULAN\VIRUS directory.

NOTE:If a virus is found in a compressed file, it will only be reported. Other scan actions - cure, rename, move, purge, delete - will not take place unless the file is decompressed. If at all possible, delete the file rather than decompress it.

Automatically Display Results

Select this option if you want to have the results of the scan displayed on the screen.

Prompt on Action

Select this option if you want to be notified before InocuLAN takes any action with infected files.

Sound Beep on Detection

Select this option if you want your workstation to beep when a virus is detected.

Scan Type

Select one of the following scan types:

Scan Type	Description
Fast Scan	Checks just the beginning and end of each file. Using Fast Scan improves scanning efficiency when processing large groups of files. *However, it is possible for a file to have a virus that may be missed by Fast Scan*. Executable files (*.EXE, *.COM, etc.) are always fully scanned.
Secure Scan	Examines the entire file. This is a thorough way to check files but is slower than running a fast scan.

Scan Type	Description
Reviewer Scan	Also examines the entire file. In addition, it searches for *virus-like* activity within files. Under unique circumstances, the Reviewer Scan may generate a false alarm. Therefore, use this scan only when the *Report Only - No Action* option is selected.

Scan Compressed Files

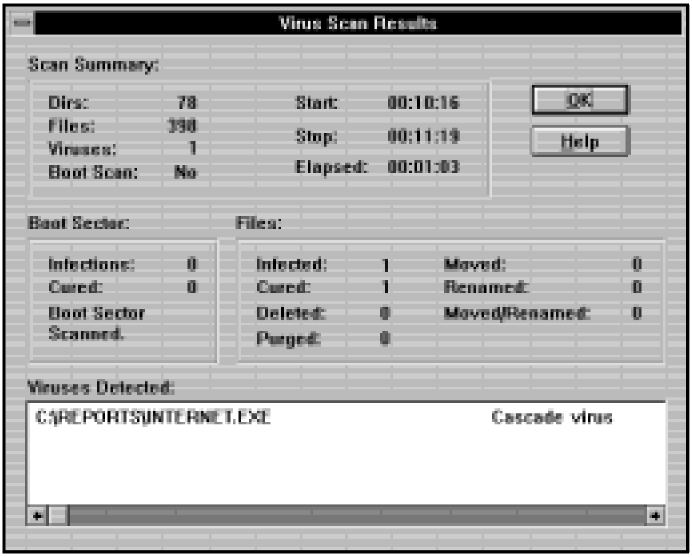
Select this option to scan compressed files. By default, InocuLAN will scan compressed files of the .ZIP and .ARJ format, as well as Microsoft compressed files. Microsoft compressed files end with an underscore, such as: STARTUP.EX_. (Note that if a Microsoft compressed file is contained *within* a ZIP file, it will not be scanned.) To add other file types, click the Add button.

3. Click OK when done.

Checking the Results of Your Scan

If you have the option *Automatically Display Results* selected, the results of your scan will appear on the screen when the scan is completed.

This screen appears when the scan is finished.



Scan Summary:

Dirs: 78
Files: 398
Viruses: 1
Boot Scan: No

Start: 00:10:16
Stop: 00:11:19
Elapsed: 00:01:03

Boot Sector:

Infections: 0
Cured: 0
Boot Sector Scanned.

Files:

Infected: 1
Cured: 1
Deleted: 0
Purged: 0
Moved: 0
Renamed: 0
Moved/Renamed: 0

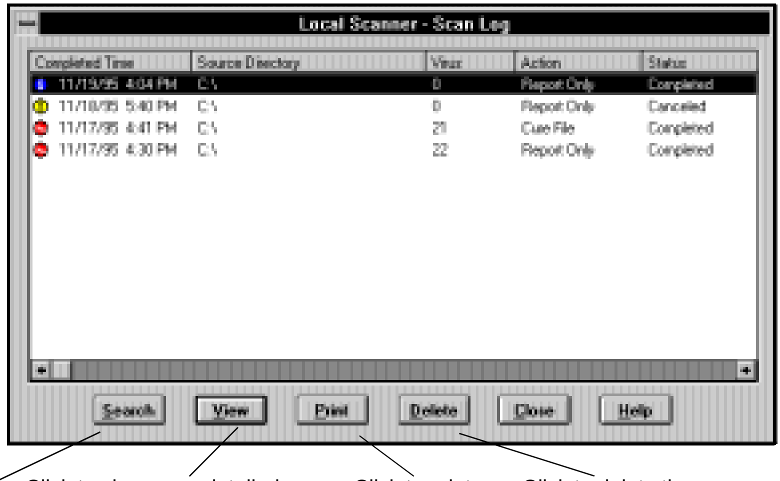
Viruses Detected:

C:\REPORTS\INTERNET.EXE Cascade virus

If you do not have this option selected, or if you want to view the results at a later time, follow the instructions on the next page.

1. Click the Reports button.

This screen displays the results of all Local Scanner jobs.



Completed Time	Source Directory	Virus	Action	Status
11/19/95 4:04 PM	C:\	0	Report Only	Completed
11/18/95 5:40 PM	C:\	0	Report Only	Canceled
11/17/95 4:41 PM	C:\	21	Cure File	Completed
11/17/95 4:30 PM	C:\	22	Report Only	Completed

Click to search the list for a specific job.

Click to view more detailed information about a job.

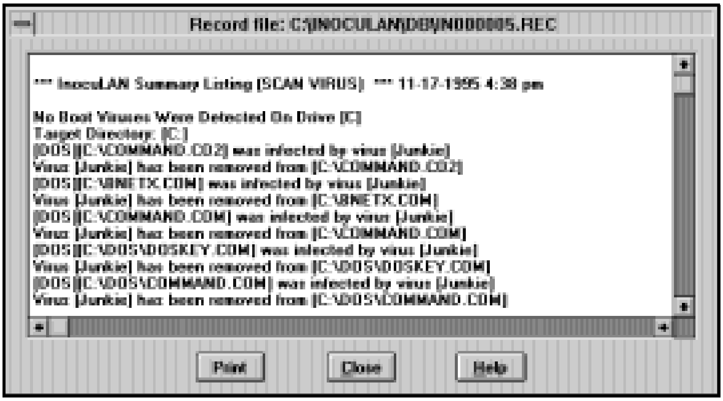
Click to print this list.

Click to delete the highlighted record.

2. Highlight the job you want to find out more information about.

3. Click View.

This screen displays detailed information about the scanning job.



```
*** InocuLAN Summary Listing [SCAN VIRUS]  *** 11-17-1995 4:38 pm

No Boot Viruses Were Detected On Drive [C]
Target Directory: [C:]
[DOS][C:\COMMAND.CO2] was infected by virus [Junkie]
Virus [Junkie] has been removed from [C:\COMMAND.CO2]
[DOS][C:\8NETX.COM] was infected by virus [Junkie]
Virus [Junkie] has been removed from [C:\8NETX.COM]
[DOS][C:\COMMAND.COM] was infected by virus [Junkie]
Virus [Junkie] has been removed from [C:\COMMAND.COM]
[DOS][C:\DOS\DOSKEY.COM] was infected by virus [Junkie]
Virus [Junkie] has been removed from [C:\DOS\DOSKEY.COM]
[DOS][C:\DOS\COMMAND.COM] was infected by virus [Junkie]
Virus [Junkie] has been removed from [C:\DOS\COMMAND.COM]
```

Using the Cheyenne AntiVirus DOS Command Line Scanner

Cheyenne AntiVirus gives you the flexibility to enter scanning commands from the MS-DOS command line, without having to start the Cheyenne AntiVirus Manager. The scan includes a check for memory resident viruses. You can also examine, backup and restore your Critical Disk Area. A command line scan uses about 110K less memory than Cheyenne AntiVirus.

Scan results will appear on screen during the course of the scan, and will also be saved in the scan log for viewing or printing at a later time.

To use the scanner, open the MS-DOS prompt in Windows. Make sure you are in the Cheyenne AntiVirus home directory. The command syntax follows:

INOCUCMD *path option*

For *path*, enter one of the following:

Path Statement	Description
DRIVE:\	Scans only the specified drive, such as C:\, or enter * to scan all local drives.
DRIVE:\DIRECTORY	Scans only the drive or drive\directory combination specified. For example, to scan the BIN directory on the C drive, enter C:\BIN.
SERVER_NAME	Scans all the volumes on the named server.

Path Statement	Description
SERVER/VOL:	Scans the named volume only on the named server. For example, to scan the PAYROLL volume on the ACCNTG server, enter ACCNTG/PAYROLL:

The `option` choices are explained below, by category.

What to scan

Option	Description
/EXE	Scan executable files only. This includes *.EXE, *.COM, *.OVL, *.PRG, *.APP, *.SYS, *.DRV and *.OVR.
/EXA	Detects boot viruses only. (Since network infection usually starts with an infected floppy disk, you can use this option to check that floppy disks are virus free before using them.)
/NCD	This option will cause Cheyenne AntiVirus to avoid scanning CD-ROM drives on your workstation. It will not skip CD-ROM drives on servers.
/NOC	Skips compressed files. By default, Cheyenne AntiVirus will scan compressed files of the .ZIP and .ARJ format, as well as Microsoft compressed files. Microsoft compressed files end with an underscore, such as STARTUP.EX_. (Note that if a Microsoft compressed file is contained *within* a ZIP file, it will not be scanned.)
/NOS	Does not scan subdirectories under the source directory.
/UPM	Scans memory up to 1M for viruses.

Scan method

Option	Description
/FST	Checks just the beginning and end of each file. Using Fast Scan improves scanning efficiency when processing large groups of files. *However, it is possible for a file to have a virus that may be missed by Fast Scan*. Executable files (*.EXE, *.COM, etc.) are always fully scanned.
/SEC	Examines the entire file. This is a thorough way to check files but is slower than running a fast scan.
/REV	Also examines the entire file. In addition, it searches for *virus-like* activity within files. Under unique circumstances, the Reviewer Scan may generate a false alarm. Therefore, use this scan only when you have not selected a scanner Action (see below).
/NS	Non-stop. Normally, a scan can be interrupted by pressing the ESC key. This option will allow the scan to ignore an ESC command.

Action upon virus detection

Option	Description
/DEL	Deletes an infected file from your workstation.
/CUR	Removes certain known viruses from infected files and restores the files to their original state. If the file cannot be cured, it will be renamed with an .AVB extension (refer to /REN below). Even if Cheyenne AntiVirus cures the file, we recommend you purge the infected file and then restore the original file.

Option	Description
/REN	Renames infected files by giving them an extension of .AVB. Files with this extension will not be scanned. If a file exists with the .AVB extension and an infected file in the same directory will result in the same file name, the .AVB extension will be changed. The extension will become .AV# and the number will be incremented for each subsequent occurrence (.AV0, .AV1, etc.). For example, an infected MOUSE.COM is renamed MOUSE.AVB and then an infected MOUSE.SYS is renamed to MOUSE.AV0.
/MOV	Moves an infected file from its current directory to the ANTIVIRUS\VIRUS directory.
/PUR	Deletes an infected file so that it cannot be recovered (for example, using the DOS UNDELETE command).
/M&R	Renames infected files by giving them a different extension and then moves them to the ANTIVIRUS\VIRUS directory.

NOTE:If a virus is found in a compressed file, it will only be reported. Other scan actions - cure, rename, move, purge, delete - will not take place unless the file is decompressed. If at all possible, delete the file rather than decompress it.

Help option

Option	Description
/HEL or /?	Displays help menu.

Reporting options

Option	Description
/LIS <report file path and name>	Generates a scanning report file using the specified path and name. For example, C:\ANTIVIRUS\INOC.RPT
/APPend	Appends the scanning report to any previously created scanning reports. Works only in conjunction with the /LIS option.
/VER	Verbose mode. This displays all information on the screen.

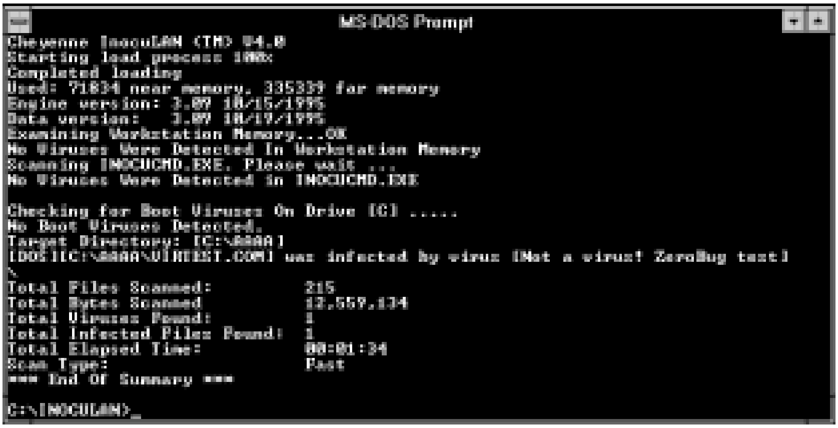
Critical Disk Area options

Option	Description
/BAK <destination path>	Backs up the Critical Disk Area to the file specified in the path. For example, to back up to the Cheyenne AntiVirus directory on drive C:, enter: INOCUCMD /BAK C:\ANTIVIRUS
/RES <source path>	Restores the Critical Disk Area using the source file specified in the path.
/EXM <backup path>	Examines the Critical Disk Area. To compare to previously backed up version, enter a backup path where it can be found.

After entering the command, messages about the progress of the scan will appear in the MS-DOS window, as shown below:

Stopping a scan

You can stop the scan at any point by pressing the ESC key. This pauses the scan and present a message asking if you wish to stop scanning. Enter Y to stop the scan, or N to continue.



```
Cheyenne InocuLAN (TM) V4.0
Starting load process 100%
Completed loading
Used: 71834 near memory, 335339 far memory
Engine version: 3.09 10/15/1995
Data version:   3.09 10/19/1995
Examining Workstation Memory...OK
No Viruses Were Detected In Workstation Memory
Scanning INOCUCMD.EXE. Please wait ...
No Viruses Were Detected in INOCUCMD.EXE

Checking for Boot Viruses On Drive [C] .....
No Boot Viruses Detected.
Target Directory: [C:\AAAA]
[DOS][C:\AAAA\VIRTEST.COM] was infected by virus [Not a virus! ZeroBug test]
\
Total Files Scanned:         215
Total Bytes Scanned          12,559,134
Total Viruses Found:         1
Total Infected Files Found:  1
Total Elapsed Time:          00:01:34
Scan Type:                   Fast
*** End Of Summary ***

C:\INOCULAN>_
```

Note that if the /NS (non-stop) option was used, pressing ESC does *not* stop the scanning process.

Automating INOCUCMD

Because it is a simple, command line program, INOCUCMD can be run automatically at start up through the AUTOEXEC.BAT file, or included in DOS batch file programs.

For example, if you wanted to backup your Critical Disk Area to your hard drive each time you booted your workstation, you could include the following command in your AUTOEXEC.BAT file:

```
C:\ANTIVIRUS\INOCUCMD  /BAK  C:\
```

NOTE:Even if you back up your Critical Disk Area at startup, it is a good idea to make a fresh backup any time you install new software, hardware, or change CMOS settings. See ‘Protecting Your Critical Disk Area’ in this Chapter for further discussion of this topic.

Command line return codes

For use with batch file processing, the following return codes apply to the command line scanner:

Error level	Meaning
Greater than 100	A virus was detected.
Greater than 2	Some kind of failure to scan.
1	A user pressed the escape key to exit the scan.
0	The scan has completed. No viruses were detected.

Sample batch file

```
@echo off
inocucmd %1 %2 %3 %4 %5 %6 %7 %8
if errorlevel 100 goto virus
if errorlevel 2 goto failure
if errorlevel 1 goto user_escape
goto no_problem
:virus
echo virus detected
goto done
:failure
echo scan failed for some reason
goto done
:user_escape
echo user hit escape
goto done
:no_problem
echo scan completed successfully
:done
```

Keeping your workstation virus-free

While you can use Cheyenne AntiVirus *just* to detect and cure problems caused by viruses, the best way to keep your workstation virus-free is to prevent viruses from gaining access to your workstation in the first place.

Cheyenne AntiVirus features

Cheyenne AntiVirus offers many features that, when used together, provide a solid barrier against viruses. These features are discussed briefly below. Detailed information about each feature can be found in this chapter.

- WIMMUNE program provides real-time protection by scanning files on your workstation for viruses each time a file is executed, accessed, or opened. It also monitors the workstation for virus-like behavior, such as unauthorized formatting of the hard disk.
- CRITICAL DISK AREA PROTECTION safeguards your workstation’s hard disk. The Critical Disk Area includes the boot sector, partition table, CMOS RAM information, and DOS system files.
- EXAMINE is a program that checks your workstation for boot viruses. The workstation’s Critical Disk Area is examined for changes, including infection and corruption.

Workstation scanners

In addition, Cheyenne AntiVirus allows you to scan your workstation by using the Workstation Scanner. Detailed information about the Workstation Scanner can be found later in this Chapter.

General suggestions

In addition to all of Cheyenne AntiVirus features, we offer the following general suggestions to help keep your workstation virus-free:

- Set all of your executable files as Read Only files. This will reduce the chance of executable files becoming infected with viruses.
- Cold-boot your workstation from write-protected, virus-free boot diskette before running Cheyenne AntiVirus.
- Use Cheyenne AntiVirus to scan floppy diskettes for viruses before copying any files from them.
- Using a product such as Cheyenne Software’s ARCServe, back up your workstation after you successfully scan the workstation for viruses. This way, if Cheyenne AntiVirus detects a file with a virus that cannot be cured, you can restore a backed up version of that file.

Real-time Monitoring with WIMMUNE

WIMMUNE, a real-time virus monitor, is a VxD (Virtual Device Driver) program that scans files on your workstation for viruses each time a file is executed, accessed, or opened. It monitors your workstation for virus-like behavior, such as unauthorized formatting of your hard disk. WIMMUNE can detect known and unknown viruses.

If WIMMUNE finds an infected file, a window will pop up on your screen to inform you. The message will display the name of the infected file and the name of the virus.

Installing and running WIMMUNE

WIMMUNE is automatically installed as part of the Windows installation process. When you start Windows, WIMMUNE will load and begin monitoring for viruses.

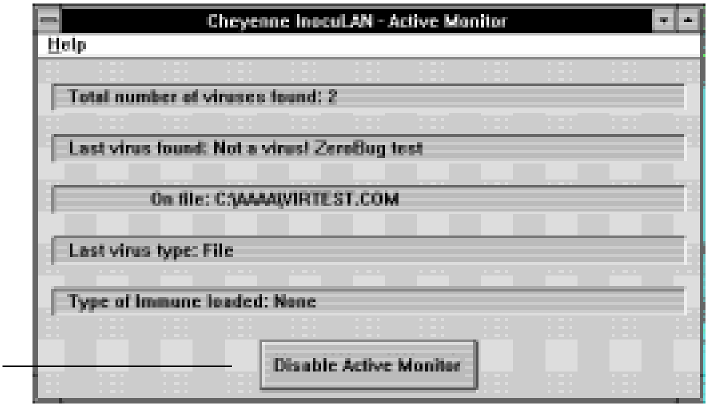
While you are in Windows, WIMMUNE's Active Monitor keeps track of viruses that are discovered on your workstation. You can view this monitor at any time by selecting *Cheyenne AntiVirus-Active Monitor* from your Windows Task List or by double-clicking the 🔍 icon when the Monitor is minimized.

If a virus is detected, a pop-up message will inform you of the virus location and name. The Active Monitor will retain the information, as shown below:

Disabling Real-time protection

You can disable the Active Monitor by clicking the *Disable Active Monitor* toggle switch on the Active Monitor window. Once clicked, the switch will read *Enable Active Monitor* and can be clicked again to reactivate the real-time protection.

WIMMUNE's Active Monitor gives information about any viruses discovered.



Total number of viruses found: 2

Last virus found: Not a virus! ZeroBug test

On file: C:\AAAA\VIRTEST.COM

Last virus type: File

Type of Immune loaded: None

You can disable the Active Monitor by clicking the toggle switch. Click it again to re-activate.

Protecting your Critical Disk Area

The Critical Disk Area of a workstation includes the Master Boot sector, Partition Table, CMOS RAM information, I/O System file, DOS system file, and Shell file (the COMMAND.COM in DOS).

The Critical Disk Area of a floppy contains the Boot sector. If the floppy is a bootable diskette, the Critical Disk Area also includes the I/O system file, DOS system file, and Shell file.

During the installation of the Cheyenne AntiVirus Manager, you had the opportunity to back up the Critical Disk Area of your workstation to a rescue diskette. In addition, this area is backed up to the Cheyenne AntiVirus home directory (the directory in which Cheyenne AntiVirus was installed).

Through Cheyenne AntiVirus, you can make a new backup of your Critical Disk Area, examine the area for viruses and changes, and restore the area from a backup.

NOTE:It is very important to maintain a current set of Critical Disk Area files for your workstation. Backups should be done on a regular basis, both to the Cheyenne AntiVirus directory and a floppy disk (if possible, all users should also back up to a central server). Any time new software is installed on your machine, CMOS information is changed, or hardware is added, it is a good idea to backup your Critical Disk Area. Your backup diskette should be write-protected, clearly labeled, and stored in a safe place.

Back Up your Critical Disk Area

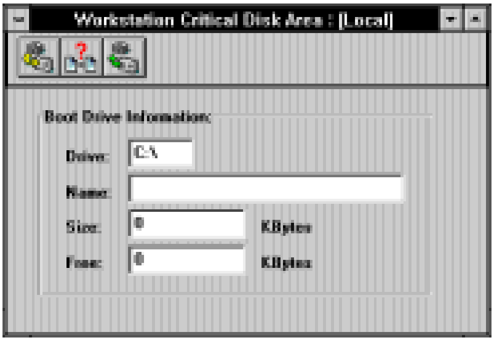
Use *Back Up* to create a rescue diskette for a workstation. The diskette you use as a rescue diskette should be a DOS system diskette. The CONFIG.SYS on this diskette must have FILES=40 or a higher number.

You should back up your Critical Disk Area anytime you change your CMOS information, change your hard disk, or upgrade your operating system.

To back up your Critical Disk Area:

1. Click the Critical Disk Area button.

   The Workstation Critical Disk Area screen appears:



Workstation Critical Disk Area : [Local]

Boot Drive Information:

Drive: C:\

Name:

Size: 0 KBytes

Free: 0 KBytes

Some basic information about your drive appears here initially.

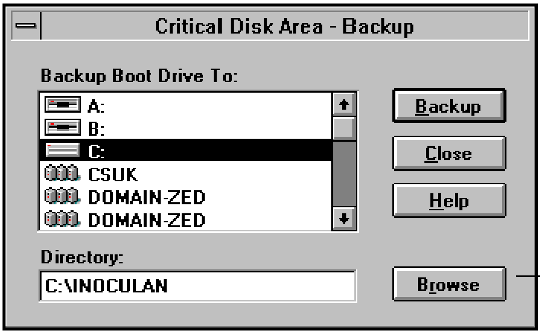
2. Click the Backup button.

3. Select a destination.

4. Click Backup.

   The Backup Activity screen will appear and the backup will begin.

Select the drive or server you wish to back up to. Note that double-clicking will start the backup process immediately.



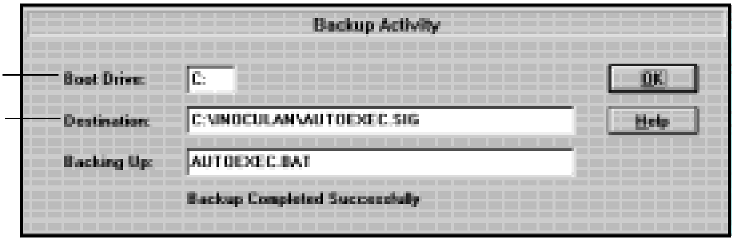
Backup Boot Drive To:
- A:
- B:
- C:
- CSUK
- DOMAIN-ZED
- DOMAIN-ZED

Directory: C:\INOCULAN

Use the Browse button to locate a specific directory.

This is the boot drive (the active partition in DOS).

This is the root of the drive selected or the Cheyenne AntiVirus home directory (if the drive selected is the drive where Cheyenne AntiVirus was installed).



Boot Drive: C:

Destination: C:\INOCULAN\AUTOEXEC.SIG

Backing Up: AUTOEXEC.BAT

Backup Completed Successfully

The information that is backed up and the files that are created are listed below:

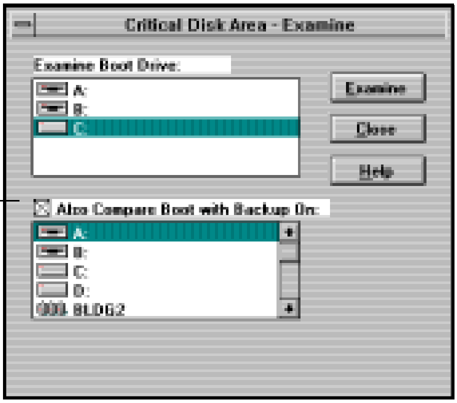
Information	File
CMOS settings	CMOS.SIG
Partition table	PARTSECT.SIG
Boot sector	BOOTSECT.SIG
DOS system file	DOS.SIG
DOS shell file	SHELL.SIG
BIOS system file	BIOS.SIG
AUTOEXEC.BAT file	AUTOEXEC.SIG
CONFIG.SYS file	CONFIG.SIG
Information about the above files and their location on the hard disk	INFO.SIG

Examine your Critical Disk Area

Use *Examine* to check your local bootable drives for viruses.

To examine your Critical Disk Area:

1. Click the Examine button on the Workstation Critical Disk Area screen.


Critical Disk Area - Examine
Examine Boot Drive:
A:
B:
C:
Examine
Close
Help
☒ Also Compare Boot with Backup On:
A:
B:
C:
D:
8LDG2

Select the drive to be examined.

Select to compare your Critical Disk Area with a backed up version.

Indicate which drive or domain contains the backed up version.

2. Select the drive to be examined.

   You can also compare your boot drive with a backup made of the Critical Disk Area.

3. Click Examine.

   The Examine Activity screen will appear and the examination will begin.

   If a virus or change is detected in the Critical Disk Area you can use a rescue diskette to restore the area. (First check to see if there is a reason for a change in the area, such as a new version of DOS.)

Restore your Critical Disk Area

Use *Restore* to recover from an infection or corruption of the Critical Disk Area.

To use the Restore function:

1. Click the Restore button on the Critical Disk screen.

2. Select the drive from which you want to restore.

   The best place to restore from is a rescue diskette. If you do not have one, your last choice should be from your local hard drive.

3. Click Restore.

   The Restore Activity screen appears and the restoration begins.

Using the command line EXAMINE utility

Cheyenne AntiVirus offers the flexibility of using an MS-DOS command line program to examine or back up your Critical Disk Area. The EXAMINE program can be run automatically at start up from the AUTOEXEC.BAT file, or included in DOS batch programs.

EXAMINE checks your workstation's hard disk for boot viruses. Your workstation's Critical Disk Area is examined for changes, including infection and corruption. The Critical Disk Area includes the boot sector, partition table, CMOS RAM information, and DOS system files.

Running EXAMINE

To execute EXAMINE:

1. Type `EXAMINE` at the DOS prompt.

   Be sure to specify the correct path for EXAMINE.

EXAMINE's options

There are several options you can use with EXAMINE.

To load EXAMINE with options:

1. Type `EXAMINE /option` at a DOS prompt.

   Be sure to specify the correct path for EXAMINE.

   The options are described in the following table:

Option	Description
/A	Accepts changes. If the Critical Disk Area has changed, this option updates the signature files.
/C	Creates new backup files that can be used to restore in the event of infection or corruption.

Option	Description
/H or /?	Displays help.
/I	Ignores changes. If the Critical Disk Area has changed, this option does not update the signature files.
/L	Uses the local (home) directory, not the directory specified in the environment variable.
/N	Does not scan memory.
/Q	Quiet mode. EXAMINE will run without being seen by the user.
/R	Restores the Critical Disk Area if it has changed.
/S	Does not check CMOS RAM information.
/1	Scans 1 Meg of memory. (The default scans 0-640K.)

Automatically running EXAMINE

During installation, you had the option of adding EXAMINE.EXE to your AUTOEXEC.BAT file. If you chose this option, the following line was added:

```
C:\ANTIVIRUS\EXAMINE
```

You may add this line to your AUTOEXEC.BAT file at any time using an appropriate text editor.

Using this command, EXAMINE will scan your Critical Disk Area each time you boot your workstation. You may add any of the EXAMINE options to the above statement. For example, you may want to ensure that you always have a current Critical Disk Area backup on your hard drive. To back up your Critical Disk Area each time you boot, modify the statement as shown below:

```
C:\ANTIVIRUS\EXAMINE /C
```

9

Chapter

USING CHEYENNE ANTIVIRUS FOR DOS

This chapter explains how to use Cheyenne AntiVirus for DOS.

In this chapter, you will learn:

Page	
9-3 ➢	How to install Cheyenne AntiVirus
9-10 ➢	Getting started with Cheyenne AntiVirus
9-24 ➢	How to scan your workstation for viruses
9-30 ➢	How to keep your workstation virus-free

9-37 ➢ How to use the EXAMINE utility

9-46 ➢ How to use the command line installation program

DOS Installation

To install the Cheyenne AntiVirus for DOS Manager:

1. Insert the Cheyenne AntiVirus Installation CD-ROM into your drive.

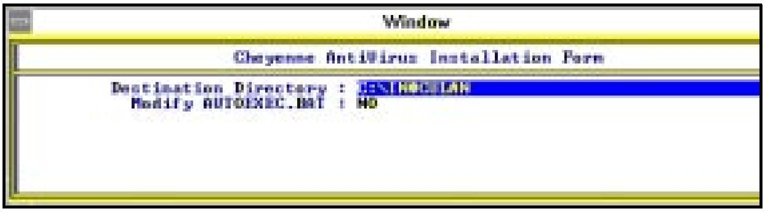
2. Change to the drive where the CD-ROM is inserted and type CD **`\DOS`** to change to the DOS directory on the CD-ROM.

3. At the DOS prompt, type **`INSTALL`** to start the installation.

   The opening screen for the Cheyenne AntiVirus installation program will be displayed while Cheyenne AntiVirus examines your workstation's Random Access Memory (RAM).

   If a virus is detected, Cheyenne AntiVirus will remove it from memory and inform you of this. (The source of the virus, such as an infected file, is not affected.)

4. Identify the path where you want to install the Cheyenne AntiVirus Manager and indicate whether or not you want your AUTOEXEC.BAT to be modified.



Cheyenne AntiVirus Installation Form

```
Destination Directory : C:\INOCULAN
  Modify AUTOEXEC.BAT : NO
```

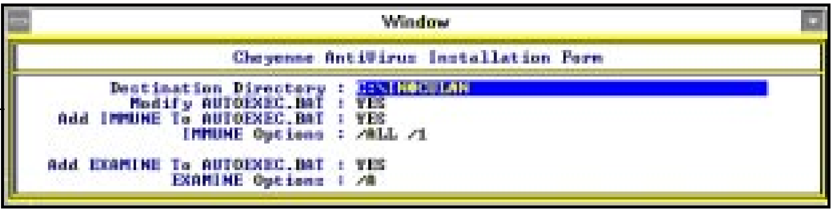
The installation program will display a default directory in which to install ANTIVIRUS. You can either accept this path or enter a different one.

5. Choose if you want to modify your AUTOEXEC.BAT file to automatically run IMMUNE and EXAMINE when you boot your PC.

   If you are installing the Cheyenne AntiVirus for DOS Manager on a workstation, you can modify your AUTOEXEC.BAT file so that Cheyenne AntiVirus's protective TSR will be loaded and/or the system integrity checker will be run when your PC is booted. If you agree to let Cheyenne AntiVirus modify your AUTOEXEC.BAT, a statement will be added to set the path of Cheyenne AntiVirus's home directory.

   If you answer YES to *Modify AUTOEXEC.BAT*, additional fields will be added to the screen.

The fields shown here may differ based on the choices you make.



```
              Cheyenne AntiVirus Installation Form

         Destination Directory : C:\INOCULAN
           Modify AUTOEXEC.BAT : YES
   Add IMMUNE To AUTOEXEC.BAT : YES
               IMMUNE Options : /ALL /1

  Add EXAMINE To AUTOEXEC.BAT : YES
              EXAMINE Options : /A
```

Add IMMUNE to AUTOEXEC.BAT

IMMUNE is a TSR that scans files on your workstation for viruses each time a file is executed, accessed, or opened. It can be set to monitor your workstation and check for virus-like behavior, such as unauthorized formatting of your hard disk. IMMUNE can detect known and unknown viruses.

There are three versions of IMMUNE: small, medium, and large. The large version detects more viruses than the small and medium versions, but uses more memory.

IMMUNE's defaults

If you do not specify any options when you load IMMUNE, it will be loaded with its defaults. The defaults are:

- The large version of IMMUNE is loaded
- IMMUNE is loaded into extended memory (if available)
- 640 K of memory will be scanned
- Only executable files will be scanned

IMMUNE Options

To change the IMMUNE defaults, enter YES in the *Add IMMUNE to AUTOEXEC.BAT* field. The *IMMUNE Options* field will appear. Press INSERT in this field to open the IMMUNE options window.

To select an option, use the up and down arrow keys to highlight it, then press F5 to mark it. Press ESC when you have finished your selections.

The options are described in the following table:

Option	Description
/ALL	Scans all files (not just executable files). This option requires a large amount of CPU resources.
/LC	Installs the large version of IMMUNE in conventional memory.
/LE	Installs the large version of IMMUNE in expanded memory. About 7K of conventional memory will also be used.
/LX	Installs the large version of IMMUNE in extended memory. About 7K of conventional memory will also be used.
/M	Installs the medium version of IMMUNE.
/N	Does not scan memory.
/NFS	Completely scans files. Without this option, IMMUNE only checks the beginning and end of files. Executable files (*.EXE, *.COM, etc.) are always fully scanned. This option requires a large amount of CPU resources.

Option	Description
/NOP	Does not scan files that are open.
/PR	Monitors your workstation for virus-like behavior, such as unauthorized formatting of your hard disk.
/HNG	LOCKS THE WORKSTATION IF A VIRUS IS FOUND. This will prevent users from ignoring a virus message. If a virus is found, the workstation will have to be rebooted before proceeding. *Be aware that any unsaved information in open files will be lost!*
/XEN	Removes Enforcement for your workstation. Use if your workstation does not log in to an Cheyenne AntiVirus domain server. For memory management purposes, this option removes the Enforcement capability from IMMUNE. This option is solely for stand-alone environments.
/XHK	Does not rehook interrupt 21 for DOS. Use if you have other TSRs that consistently rehook to this interrupt.
/XLN	Disables all network communication features. Use for stand-alone workstations. This option reduces the size of the small version of IMMUNE.
/Q	Does not display messages while IMMUNE is loading.
/S	Loads the small version of IMMUNE.
/1	Scans 1 Meg of memory.

Add EXAMINE To AUTOEXEC.BAT

EXAMINE is a program that checks your workstation for changes to the Critical Disk Area. The Critical Disk Area includes the master boot sector, partition table, CMOS RAM information, and DOS system files.

To select the EXAMINE options, enter YES in the *Add EXAMINE to AUTOEXEC.BAT* field. The *EXAMINE Options* field will appear. Press INSERT in this field to open the EXAMINE options window.

To select an option, use the up and down arrow keys to highlight it, then press F5 to mark it. Press ESC when you have finished your selections.

The options are described in the following table:

Option	Description
/A	Accepts changes. If the Critical Disk Area has changed, this option updates the signature files.
/I	Ignores changes. If the Critical Disk Area has changed, this option does not update the signature files.
/N	Does not scan memory.
/Q	Quiet mode. Does not display messages when EXAMINE is running.
/S	Does not check CMOS RAM information.
/1	Scans 1 Meg of memory. (The default scans 0-640K.)

6. Press F2 when the form is complete.

7. Select **YES** to confirm the installation.

   The lower part of the screen displays the installation activity.

   First, Cheyenne AntiVirus files are copied.

   Second, if you chose to modify your AUTOEXEC.BAT, the file will be modified to load IMMUNE and/or EXAMINE. A statement that sets the path of Cheyenne AntiVirus's home directory is also added. The original file is saved in Cheyenne AntiVirus's home directory as AUTOEXEC.BAK.

If you chose not to modify your AUTOEXEC.BAT, an AUTOEXEC.INO file is created in Cheyenne AntiVirus's home directory. This file is a copy of your current AUTOEXEC.BAT with the recommended modifications that should be made. You can examine this file after the installation, and if you want, you can substitute this file for the AUTOEXEC.BAT you are currently using or you can add these statements to your current AUTOEXEC.BAT.

The AUTOEXEC.INO will contain the following additional statements:

```
SET ANTIVIRUS=C:\ANTIVIRUS
C:\ANTIVIRUS\EXAMINE
C:\ANTIVIRUS\IMMUNE.EXE
```

Third, the Critical Disk Area is backed up to the destination directory. This is done so that recovery from a viral infection or other corruption of this disk area can be accomplished, if necessary.

8. Indicate if you want to create a rescue diskette.

   A rescue diskette is a backup of the Critical Disk Area. While you can back up your Critical Disk Area once Cheyenne AntiVirus is loaded on your workstation, we strongly recommend that you take the time to perform this step now. This extra precaution may be a life saver if a virus is encountered.

   The diskette you use should be a DOS system diskette with a CONFIG.SYS file that has FILES=40 or a higher number. Write-protection should be added after the rescue diskette is created.

Once the rescue diskette is created, installation of the Cheyenne AntiVirus Manager is complete. You will see a message that says Cheyenne AntiVirus was installed successfully.

Setting the environment variable

If you did not let Cheyenne AntiVirus modify the AUTOEXEC.BAT file, you should minimally add the following statement to the AUTOEXEC.BAT file in order to set the path for Cheyenne AntiVirus:

```
SET ANTIVIRUS=path
```

where `path` is Cheyenne AntiVirus's home directory (such as C:\ANTIVIRUS).

Starting Cheyenne AntiVirus

To load the Cheyenne AntiVirus for DOS Manager on your workstation:

1. Change to the directory where the Cheyenne AntiVirus for DOS Manager is installed.

2. Type **`Cheyenne AntiVirus`** to start Cheyenne AntiVirus for DOS.

   If Cheyenne AntiVirus was installed using the Windows installation program, you can load Cheyenne AntiVirus by double clicking the Cheyenne AntiVirus icon in the Cheyenne AntiVirus program group.

   The Cheyenne AntiVirus program begins by checking the workstation's memory. If there are no viruses detected in RAM and ANTIVIRUS.EXE is not infected, Cheyenne AntiVirus's Available Topics menu will be displayed.

   If Cheyenne AntiVirus detects a virus loaded in memory, Cheyenne AntiVirus will remove the virus and display a message showing the number of viruses that were neutralized. Then, the Available Topics menu will appear.

NOTE: Even though Cheyenne AntiVirus has removed the virus(es) from memory, you should reboot your workstation with a write-protected, clean boot diskette (such as the original operating system diskette) before continuing with Cheyenne AntiVirus for DOS.

The basic Cheyenne AntiVirus for DOS screens

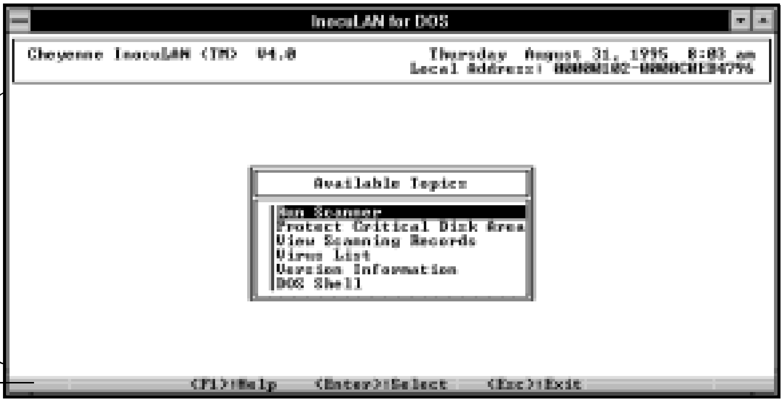
There are three basic screens used in Cheyenne AntiVirus for DOS:

- Menus
- Lists
- Forms

Regardless of the type of screen, every screen has the same basic format.

The header contains basic information about your version of Cheyenne AntiVirus for DOS and your workstation. The footer lists all of the keys that are available on the current screen.

The following is the Cheyenne AntiVirus for DOS main menu.



```
Cheyenne InocuLAN (TM)  V4.0           Thursday  August 31, 1995  8:03 am
                                  Local Address: 00000102-0000C0E84795

                    Available Topics
                    Run Scanner
                    Protect Critical Disk Area
                    View Scanning Records
                    Virus List
                    Version Information
                    DOS Shell

            <F1>:Help    <Enter>:Select    <Esc>:Exit
```

This section of the screen will vary depending upon where you are in Cheyenne AntiVirus for DOS.

These are the keys that are available on this screen.

Menus

The Cheyenne AntiVirus for DOS Manager is menu-driven.

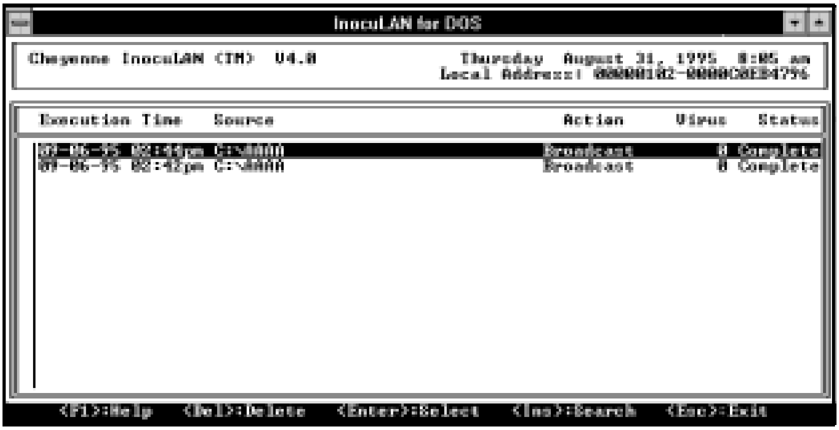
To select a menu option:

1. Use the arrow keys to highlight the desired option.

2. Press ENTER (or click the left mouse button).

Lists

A list is similar to a menu. It can be used to view information (as in the case of Cheyenne AntiVirus's Virus List), or, more commonly, to select one or more items from a group of options.



```
InocuLAN for DOS

Cheyenne InocuLAN (TM)  V4.0            Thursday  August 31, 1995  8:05 am
                                 Local Address: 00000102-0000C0EB4796

 Execution Time   Source                         Action      Virus   Status
09-06-95 02:44pm C:\AAAA                         Broadcast       0 Complete
09-06-95 02:42pm C:\AAAA                         Broadcast       0 Complete

   <F1>:Help   <Del>:Delete   <Enter>:Select   <Ins>:Search   <Esc>:Exit
```

To select one item from a list:

1. Use the arrow keys to highlight the desired item.

2. Press ENTER (or click the left mouse button).

If a list allows you to select multiple items:

1. Use the arrow keys to highlight the desired item.

2. Press F5 to mark the item.

3. Repeat steps 1 and 2 until all of your items have been selected.

Forms

A form is used to enter data into fields.

Whenever possible, default values appear in the fields when a form is initially displayed.

Forms have three types of fields:

- Text Entry fields - allow you to enter information
- Toggle fields - allow you to select from two options
- List fields - allow you to select one or more items from a group of options

Details about entering information into each of these types of fields follows.

Entering information into fields

To enter information into any type of field, you must place the cursor in that field.

To place the cursor in a field:

1. Highlight the field.

2. Press ENTER (or click the left mouse button).

Text entry fields

Some text entry fields allow you to type in the information, such as a date or time.

Other text entry fields, such as those fields that require a valid workstation path, allow you to build the path by selecting from lists of drives and directories.

To access these lists from within one of these fields:

1. Press the INSERT key (or click the left mouse button).

2. Highlight an entry from the list.

3. Press ENTER (or click the left mouse button).

   The next level down in the directory tree will be displayed.

4. Repeat steps 2 and 3 until the desired path is displayed.

   You can use the “..” option to remove the last entry you chose. This will return you to the previous level of the directory tree. (This is similar to the DOS command CD.. which is used to return to one level higher in the directory tree.)

You can specify a particular file name by typing a backslash and then the file name.

5. Press ESC (or click the right mouse button).

Toggle fields

Toggle fields allow you to select from two options.

To select an option:

1. Highlight the field and press ENTER.
2. Use the left/right arrow keys or a corresponding letter on your keyboard to select an option (or click the left mouse button).

List fields

List fields allow you to select one or more items from a group of options.

To select one item from a list:

1. Use the arrow keys (or mouse) to highlight the desired item.
2. Press ENTER (or click the left mouse button).

If a list allows you to select multiple items:

1. Use the arrow keys (or mouse) to highlight the desired item.
2. Press F5 to mark the item.
3. Repeat steps 1 and 2 until all of your items have been selected.

Keys used in Cheyenne AntiVirus for DOS

The keys used by Cheyenne AntiVirus for DOS are described in the table below:

Key	Meaning	Function
F1	HELP	Accesses Cheyenne AntiVirus's online help. Press F1 a second time to display a list of keys that are used with Cheyenne AntiVirus for DOS.
F2	DONE	Executes a form and processes the information.
F3	MODIFY	Allows you to edit an item.
F5	MARK	Flags multiple items for selection.
F6	MARK ALL	Selects all items in a list. When viewing the Activity Log, this key captures the log in a file or sends it to a printer.
F7	SEARCH	Allows you to search a string. In a field, this key lets you cancel the changes you entered.
ENTER	SELECT	Selects a highlighted item, accepts the information you entered, and confirms selections.
ESC	ESCAPE	Returns you to the previous screen or exits you from Cheyenne AntiVirus for DOS.
INSERT	INSERT	Adds an additional item to a list or adds information to a field. When used with forms, this key displays path information.
DELETE	DELETE	Deletes an item from a list or deletes information from a field.

Key	Meaning	Function
PAGE UP	PAGE UP	Returns to the previous page of a help screen, list, or file.
PAGE DOWN	PAGE DOWN	Advances to the next page of a help screen, list, or file.
ARROWS	CURSOR CONTROL	Moves the cursor around a menu, list, form, or field. This key can also be used to toggle between options within a toggle field.
BACKSPACE	BACKSPACE	Deletes the character to the left of the cursor.
TAB	TAB	Moves the cursor around a form.

Using a mouse with Cheyenne AntiVirus for DOS

Cheyenne AntiVirus for DOS allows you to use a mouse for many functions.

In order to use a mouse with Cheyenne AntiVirus, a mouse driver must be loaded on your workstation. Refer to the manual that came with your mouse for information about installing a mouse driver on your workstation.

If a mouse driver is loaded, the mouse pointer (a character block) appears on your screen to the right of the Available Topics menu when Cheyenne AntiVirus for DOS is started.

Left mouse button

Use the left mouse button to select menu and list items. You can also move from field to field in a form and change the selection in a toggle field using the left mouse button.

Right mouse button

The right mouse button works like the ESCAPE key. It returns you to the previous screen or exits you from Cheyenne AntiVirus for DOS.

Online help in Cheyenne AntiVirus for DOS

Cheyenne AntiVirus for DOS offers online help on every screen.

If you are on a menu or a list, the online help will display general information about that screen.

If you are on a form, the online help will display information about the specific field that you are in.

Accessing online help

To access online help from any Cheyenne AntiVirus for DOS menu, list, or form:

1. Press F1.

   Press F1 a second time to display a list of keys that are used with Cheyenne AntiVirus for DOS.

Version information

You can display information about the version of Cheyenne AntiVirus for DOS installed on your workstation.

Displaying version information for your workstation

To display version information for your workstation:

1. Select Version Information from the Available Topics menu off of the main menu.

Temporarily exiting to DOS

While you are using Cheyenne AntiVirus for DOS you can temporarily exit and go to DOS to execute DOS commands.

While Cheyenne AntiVirus for DOS is loaded and running on a workstation, IMMUNE is disabled. This eliminates double scanning operations.

Instructions for exiting to DOS

To temporarily exit to DOS:

1. Select DOS Shell from the Available Topics menu.

   You will be brought to the DOS prompt.

2. Type **`Exit`** when you are ready to return to Cheyenne AntiVirus for DOS.

   If the path to your COMMAND.COM file is incorrect (for example, your user login script set the path, but your server connection has been lost) you may need to use the DOS command SET COMSPEC to help Cheyenne AntiVirus for DOS locate your COMMAND.COM.

   The following examples illustrate how you might use the SET COMSPEC command:

   ```
   SET COMSPEC=D:\COMMAND.COM
   SET COMSPEC=C:\COMMAND.COM
   SET COMSPEC=C:\BIN\COMMAND.COM
   ```

Virus list

You can display a list of the viruses that Cheyenne AntiVirus for DOS can detect. You can also print this list.

Displaying the virus list

To display the list:

1. Select Virus List from the Available Topics menu.

   The list is displayed.

Searching for a specific virus

You can search the virus list for a specific virus name.

To search:

1. Press F7 to bring up the search window.
2. Enter the virus name you want to find.
3. Press ENTER.

   If you want to search for the same text again, press SHIFT and F7 together.

Printing the virus list

You can create a report from this list. This report can be sent directly to a printer or it can be captured in a file and printed at a later time.

To create a report:

1. Press F6.
2. Enter a path and file name for the report.

   Enter the printer port (LPT1, for example) to send the report to the printer.

To capture the report to a file, you can press INSERT to display available drives and directories.

Using the Run Scanner

The Run Scanner scans files on your workstation.

Instructions for using the Run Scanner

Follow the instructions below for using the Run Scanner:

1. Select Run Scanner from the Available Topics menu on the main menu.

   The Scanner Form will be displayed.

2. Enter information on the Scanner Form.

Source Directory

Enter the directory where scanning should start. You can select an entire workstation drive or a specific directory. An asterisk (*) indicates that all local hard drives will be scanned.

Press INSERT twice to display available drives, directories, and subdirectories.

Traverse Directory

Enter `Yes` to scan all subdirectories under the source directory or `No` to scan just the source directory.

Report File

Enter a path and file name for a report of the scan. You can press the INSERT key to help select the path.

The report will show the number of files and directories scanned, the number of infected files found, and the action taken. If an infected file is found, the virus responsible will also be listed.

Append Report File

Indicate if you want the report to append to the report file you named in the previous field. If you answer `No`, an existing report file will be overwritten.

Skip CD-ROM

Selecting this option will cause Cheyenne AntiVirus to *not* scan CD-ROM drives on your workstation. Note that this field only appears if you have a CD-ROM drive on your machine.

File Selection

Press INSERT twice to select specific types of DOS files for scanning.

You can select all files or a selection of executable files. If you select *EXECUTABLE FILES,* you can further define which files to scan by their extensions.

If you select *ALL FILE*S, the Files Excluded list will be displayed.

You can exclude specific files or directories from being scanned. For example, you might want to exclude all files in a directory used for research purposes only.

To specify a file or directory, press ENTER. You can then press INSERT to choose from available servers, drives, volumes, directories, and subdirectories.

You can use wildcards. For example, you could use a wildcard to exclude files with a specific extension (such as *.BAK).

If you want to specify an entire directory, type `\*.*` after the directory name (for example: `WRITER/SYS:\MANUAL\*.*`).

Scan Type

Select one of the following Scan Types:

Scan Type	Description
Fast Scan	Checks just the beginning and end of each file. Using Fast Scan improves scanning efficiency when processing large groups of files. *However, it is possible for a file to have a virus that may be missed by Fast Scan*. Executable files (*.EXE, *.COM, etc.) are always fully scanned.
Secure Scan	Examines the entire file. This is a thorough way to check files but is slower than running a fast scan.
Reviewer Scan	Also examines the entire file. In addition, it searches for *virus-like* activity within files. Under unique circumstances, the Reviewer Scan may generate a false alarm. Therefore, use this scan only when the *Report Only* option is selected.

Scan Compressed Files

Select this option for Cheyenne AntiVirus to scan compressed files. By default, Cheyenne AntiVirus scans files of the ZIP and ARJ format, as well as Microsoft compressed files. Microsoft compressed files end with an underscore, such as: STARTUP.EX_. (Note that if a Microsoft compressed file is contained *within* a ZIP file, it will not be scanned.) To add other file types, press Insert in the *Compressed File Extensions* field.

Action Upon Virus Detection

Press ENTER to display a list of options. Regardless of which option you choose, a message will be broadcast when a virus is detected.

Option	Description of Action
Report Only	Displays an on-screen report that lists the infected files and the virus that was detected. This information also appears in the Scanning Report.
Delete File	Deletes an infected file from your workstation.
Cure File	Removes certain known viruses from infected files and restores the files to their original state. If the file cannot be cured, it will be renamed with an .AVB extension (refer to ‘Rename File’ below). Even if Cheyenne AntiVirus cures the file, we recommend you purge the infected file and then restore the original file.
Move File	Moves an infected file from its current directory to the ANTIVIRUS\VIRUS directory.
Rename File	Renames infected files by giving them an .AVB extension. Files with this extension will not be scanned. If a file exists with the.AVB extension and an infected file in the same directory will result in the same file name, the.AVB extension will be changed. The extension will become.AV# and the number will be incremented for each subsequent occurrence (.AV0,.AV1, etc.). For example, an infected MOUSE.COM is renamed MOUSE.AVB and then an infected MOUSE.SYS is renamed to MOUSE.AV0.
Purge File	Deletes an infected file so that it cannot be recovered (for example, using DOS’s Undelete).

Option	Description of Action
Move and Rename File	Renames infected files by giving them a different extension and then moves them to the ANTIVIRUS\VIRUS directory.

NOTE:If a virus is found in a compressed file, it will only be reported. Other scans actions - cure, rename, move, purge, delete - will not take place unless the file is decompressed. If at all possible, delete the file rather than decompress it.

3. Press F2 when the form is complete.

4. Answer **Yes** to confirm.

   The scanner activity will be displayed on your screen.

Virus recovery procedures

If the Local Scanner locates a virus, you must begin proper virus recovery procedures.

Checking the results of your scan

Follow the instructions below to see the results of the Run Scanner job:

1. Select View Scanning Records from the Available Topics menu.

   This screen displays the results of scans run with the Run Scanner.

2. Highlight the job you want to find out more information about.

3. Press ENTER.

DOS command line scanner

Cheyenne AntiVirus gives you the flexibility to enter scanning commands from the DOS command line. You can also examine, backup and restore your Critical Disk Area.

Keeping your workstation virus-free

While you can use Cheyenne AntiVirus for DOS *just* to detect and cure problems caused by viruses, the best way to keep your workstation virus-free is to prevent viruses from gaining access to your workstation in the first place.

Cheyenne AntiVirus for DOS features

Cheyenne AntiVirus for DOS offers many features that, when used together, provide a solid barrier against viruses. These features are discussed briefly below. Detailed information about each feature can be found in this chapter.

- IMMUNE is a TSR that scans files on a workstation for viruses each time a file is executed, accessed, or opened. It can also be set to monitor the workstation for virus-like behavior, such as unauthorized formatting of the hard disk. IMMUNE can be used on all workstations, even workstations that do not have an Cheyenne AntiVirus Manager installed.
- EXAMINE is a program that checks a workstation for boot viruses. The workstation's Critical Disk Area is examined for changes, including infection and corruption.
- CRITICAL DISK AREA PROTECTION safeguards a workstation's hard disk. The Critical Disk Area includes the master boot sector, partition table, CMOS RAM information (system configuration information for your AT or

compatible computer), and DOS system files.

Run scanner

In addition, Cheyenne AntiVirus allows you to scan your workstation by using the Run Scanner. Detailed information about these scanners can be found later in this Chapter, “Scanning and Safeguarding your Workstation with Cheyenne AntiVirus for DOS.”

General suggestions

In addition to all of the Cheyenne AntiVirus for DOS features, we offer the following general suggestions to help keep your workstation virus-free:

- Set all of your executable files as Read Only files. This will reduce the chance of executable files becoming infected with viruses.
- Cold-boot your workstation from a virus-free boot diskette before running Cheyenne AntiVirus for DOS.
- Use Cheyenne AntiVirus for DOS to scan floppy diskettes for viruses before copying any files from them.
- Back up your workstation after you successfully scan the workstation for viruses. This way, if Cheyenne AntiVirus for DOS detects a file with a virus that cannot be cured, you can restore a backed up version of that file. (Users of Cheyenne Software’s ARCserve can use Cheyenne AntiVirus for DOS to perform a virus check prior to backing up information.)

Using IMMUNE

IMMUNE is a TSR that scans files on your workstation for viruses each time a file is executed, accessed, or opened. It can be set to monitor your workstation for virus-like behavior, such as unauthorized formatting of your hard disk. IMMUNE can detect known and unknown viruses.

There are three versions of IMMUNE:

- Small - uses 11-13 K conventional memory
- Medium - uses 30 K conventional memory
- Large - memory usage varies depending upon where IMMUNE is loaded:
- Loaded in conventional memory uses 109 K conventional memory.
- Loaded in extended memory uses 7 K conventional memory and 125 K extended memory.
- Loaded in expanded memory uses 7 K conventional memory, 61 K extended memory, and 64 K expanded memory.

The large version detects more viruses than the small and medium versions, but uses more memory. The large version detects all of the viruses listed in the Virus List.

You can specify which version of IMMUNE you want to use when you load IMMUNE. There are also a number of options you can use when loading IMMUNE. They are discussed on page 9-34.

If IMMUNE finds an infected file, a window will pop up on your screen to inform you. The message will display the name of the infected file and the name of the virus.

Loading IMMUNE

Using the AUTOEXEC.BAT

When Cheyenne AntiVirus for DOS was installed on your workstation, IMMUNE was copied to Cheyenne AntiVirus's home directory (where Cheyenne AntiVirus for DOS is installed). If your workstation's AUTOEXEC.BAT was modified during the installation, IMMUNE will be loaded each time the workstation is booted.

If the AUTOEXEC.BAT was not modified but you want to use it to load IMMUNE, you will have to add a command to the AUTOEXEC.BAT. The command must specify the path where IMMUNE is located. For example, if your Cheyenne AntiVirus for DOS home directory is the ANTIVIRUS directory on your C drive, your statement would look like the following:

```
C:\ANTIVIRUS\IMMUNE.EXE
```

Manually loading IMMUNE

You can manually load IMMUNE from a DOS prompt. If you do this, each time the workstation is rebooted, IMMUNE will have to be manually loaded again.

Loading IMMUNE on a workstation without Cheyenne AntiVirus

If a workstation does not have Cheyenne AntiVirus installed, you can still load IMMUNE. The only files needed to run IMMUNE are:

- IMMUNE.DAT
- INMEM.DAT
- IMMUNE.EXE
- MIMMUNE.DAT
- SIMMUNE.DAT

Loading IMMUNE on an OS/2 workstation

IMMUNE must be loaded in a DOS box on an OS/2 workstation. Each time you open a DOS box, you must load IMMUNE. This can be done automatically by adding a command to the AUTOEXEC.BAT. The command must specify the path where IMMUNE is located.

Loading IMMUNE without any options

The command to load IMMUNE is:

1. Type **`IMMUNE`**.

   Be sure to specify the correct path for IMMUNE.

IMMUNE's defaults

If you do not specify any options when you load IMMUNE, it will be loaded with its defaults. The defaults are:

- The large version of IMMUNE is loaded
- IMMUNE is loaded into extended memory (if available)
- 640 K of memory will be scanned
- Only executable files will be scanned

IMMUNE's options

There are several options you can use with IMMUNE. To load IMMUNE with options:

1. Type **`IMMUNE /option1 /option2`**...

   Be sure to specify the correct path for IMMUNE.

   You can specify one or more options.

   The options are described in the following table:

Option	Description
/ALL	Scans all files (not just executable files).
/DIS	Disables IMMUNE without unloading it.

Option	Description
/ENA	Enables IMMUNE (if it is disabled).
/H or /?	Displays help.
/LC	Installs the large version of IMMUNE in conventional memory.
/LE	Installs the large version of IMMUNE in expanded memory. About 7 K of conventional memory will also be used.
/LX	Installs the large version of IMMUNE in extended memory. About 7 K of conventional memory will also be used.
/M	Installs the medium version of IMMUNE.
/N	Does not scan memory.
/NFS	Completely scans files. Without this option, IMMUNE only checks the beginning and end of files. Executable files (*.EXE, *.COM, etc.) are always fully scanned. This option requires a large amount of CPU resources.
/HNG	Locks the workstation if a virus is found. This will prevent users from ignoring a virus message. If a virus is found, the workstation will have to be rebooted before proceeding. *Be aware that any unsaved information in open files will be lost!*
/NOP	Does not scan files that are open.
/NT	Returns an errorlevel of 1 if IMMUNE is not loaded. (This option can be used in a batch file or system login script.) See the next page for more information.
/NTC	Updates the virus signature file if it is out of date.
/NTL	Returns an errorlevel of 1 if the large version of IMMUNE is not loaded. (This option can be used in a batch file or system login script.) See the next page for more information.

Option	Description
/PR	Monitors your workstation for virus-like behavior, such as unauthorized formatting of your hard disk.
/XEN	Removes Enforcement for your workstation. Use if your workstation does not log in to an Cheyenne AntiVirus domain server. For memory management purposes, this option removes the Enforcement capability from IMMUNE. This option is solely for stand-alone environments.
/XHK	Does not rehook interrupt 21 for DOS. Use if you have other TSRs that consistently rehook to this interrupt. Use this option if you are having a problem with IMMUNE and another TSR.
/XLN	Disables all network communication features. Use for stand-alone workstations. Reduces the size of IMMUNE.
/Q	Does not display messages while IMMUNE is loading.
/S	Loads the small version of IMMUNE.
/U	Unloads IMMUNE from memory. If a TSR is loaded after IMMUNE, IMMUNE will not unload.
/1	Scans 1 Meg of memory.

Using the EXAMINE Program

Cheyenne AntiVirus offers the flexibility of using an MS-DOS command line program to quickly and efficiently examine or back up your Critical Disk Area. The EXAMINE program can be run automatically at start up from the AUTOEXEC.BAT file, or included in DOS batch programs. Whichever way you run it, the EXAMINE program serves as your first line of defense in checking for viruses on your hard drive.

How EXAMINE works

The EXAMINE utility performs two major missions: it allows the user to quickly determine, at the point of bootup, that there are no viruses, and then compares your current Critical Disk Area information with the archived Critical Disk Area files for any differences on your computer.

Your workstation’s Critical Disk Area is examined for changes, including infection and corruption. In the first stage, EXAMINE scans the Critical Disk Area, including the boot sector, partition table, CMOS memory, and DOS system files, assuring that your PC starts up. In the second stage, EXAMINE looks at the stored rescue diskette files on your hard drive and compares them with your current workstation configuration to alert you of any changes.

Running EXAMINE

To execute EXAMINE:

1. Type **`EXAMINE`** at the DOS prompt.

   Be sure to specify the correct path for EXAMINE.

   You will see the following at your DOS command line:

```
C:\progra~1\cheyenne\inoculan>examine
Cheyenne AntiVirus V4.0
Copyright 1997 Computer Associates
International, Inc.
and/or its subsidiaries. All Rights Reserved.
Home Directory
C:\src\examine
Testing Extended Memory            OK
Engine version                     3.36
Data version                       3.36
Starting load process              OK
Scanning memory to 640k            OK
Scanning C:\SRC\EXAMINE\EXAMINE.EXE OK
Scanning BIOS System File          OK
Scanning DOS System File           OK
Scanning DOS Shell File            OK
Scanning Boot On Drive [C]         OK
Scanning Boot On Drive [D]         OK
Scanning Boot On Drive [E]         OK
CMOS Settings                      OK
```

EXAMINE Actions

There are several options you can implement with EXAMINE.

To load EXAMINE with options:

1. Type **`EXAMINE /option`** at the DOS prompt.

   Be sure to specify the correct path for EXAMINE.

   The options are described in the following table:

Option	Description
/A	Accepts changes. If the Critical Disk Area has changed, this option updates the signature files.
/C	Creates new backup files that can be used to restore in the event of infection or corruption.

Option	Description
/H or /?	Displays help.
/I	Ignores changes. If the Critical Disk Area has changed, this option does not update the signature files.
/L	Uses the local (home) directory, not the directory specified in the environment variable.
/N	Does not scan memory.
/Q	Quiet mode. EXAMINE will run without being seen by the user.
/R	Restores the Critical Disk Area if it has changed.
/S	Does not check CMOS RAM information.
/1	Scans 1 Meg of memory. (The default scans 0-640K.)

Using this command, EXAMINE will scan your Critical Disk Area each time you boot your workstation. You may add any of the EXAMINE options to the above command line statement. For example, you may want to ensure that you always have a current Critical Disk Area backup on your hard drive. To back up your Critical Disk Area each time you boot, modify the statement as shown below:

```
C:\ANTIVIRUS\EXAMINE /C
```

EXAMINE at work

Let’s say, for example, that you have added a new hard drive to your machine.

The next time you run EXAMINE at bootup, you see at the DOS command line that the CMOS settings have been changed, as in this example:

```
CMOS Settings                       CHANGED

    What do you want to do with the CMOS Settings?

    (A) Accept  'I know why the settings changed
and wish to save them.'

    (I) Ignore  'Keep old settings and remind me
next time.'

    (R) Restore 'Restore old settings.'

    (Q) Quit   'I wish to Quit and verify why these
settings changed.'

    a

    Accepted
```

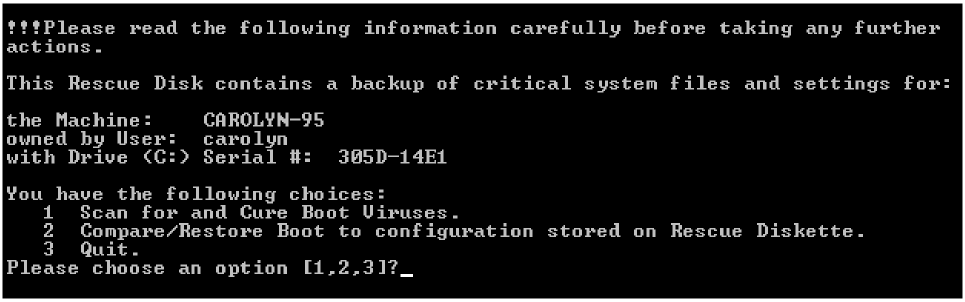
If you choose Accept, you will be prompted later to update your rescue diskette.

If you choose Restore, EXAMINE will grab the existing backed up rescue diskette files from the INOCULAN directory on your hard disk and restore your computer configuration.

WARNING: Do not restore anything without being sure that the files you are restoring from are the correct ones for configuring your specific workstation. Otherwise, your Windows 95 machine may not boot properly.

If you have accepted new changes or created a new set of backup files, you will have the opportunity to save these files to a floppy disk. If you insert the rescue diskette, you will then see a prompt asking you whether you wish to overwrite your current rescue diskette.

You will also see the following information to help you verify that this is the proper rescue diskette for this machine:



```
!!!Please read the following information carefully before taking any further
actions.

This Rescue Disk contains a backup of critical system files and settings for:

the Machine:    CAROLYN-95
owned by User:  carolyn
with Drive (C:) Serial #:  305D-14E1

You have the following choices:
   1  Scan for and Cure Boot Viruses.
   2  Compare/Restore Boot to configuration stored on Rescue Diskette.
   3  Quit.
Please choose an option [1,2,3]?_
```

Protecting your Critical Disk Area

The Critical Disk Area of a workstation includes the boot sector, Partition Table, CMOS RAM information, I/O system file, DOS system file, and Shell file (the COMMAND.COM in DOS).

The Critical Disk Area of a floppy contains the Boot sector. If the floppy is a bootable diskette, the Critical Disk Area also includes the I/O system file, DOS system file, and Shell file.

It is very important to maintain a current set of Critical Disk Area files for your workstation.

During the installation of the Cheyenne AntiVirus for DOS Manager, you had the opportunity to back up the Critical Disk Area of your workstation to a rescue diskette. In addition, this area is backed up to the Cheyenne AntiVirus for DOS home directory (the directory in which Cheyenne AntiVirus for DOS was installed).

Through Cheyenne AntiVirus for DOS, you can make a new backup of your Critical Disk Area, examine the area for viruses and changes, and restore the area from a backup.

NOTE:It is very important to maintain a current set of Critical Disk Area files for your workstation. Backups should be done on a regular basis, both to the Cheyenne AntiVirus directory and a floppy disk (if possible, all users should also back up to a central server). Any time new software is installed on your machine, CMOS information is changed, or hardware is added, it is a good idea to back up your Critical Disk Area.

Your backup diskette should be write-protected, clearly labeled, and stored in a safe place.

Back Up your Critical Disk Area

Use *Back Up* to create a rescue diskette for a workstation. The diskette you use as a rescue diskette should be a DOS system diskette. The CONFIG.SYS on this diskette must have FILES=40 or a higher number.

You should back up your Critical Disk Area anytime you change your CMOS information, change your hard disk, or upgrade your operating system.

To back up your Critical Disk Area:

1. Select Protect Critical Disk Area from the Available Topics menu.

2. Select Back Up from the Critical Area Options menu.

3. Select a destination from the list.

4. Press ENTER.

   The Back Up Activity screen will appear and the back up will begin.

The information that is backed up and the files that are created are listed below:

Information	File
CMOS settings	CMOS.SIG
Partition table	PARTSECT.SIG
Boot sector	BOOTSECT.SIG
DOS system file	DOS.SIG
DOS shell file	SHELL.SIG
BIOS system file	BIOS.SIG
AUTOEXEC.BAT file	AUTOEXEC.SIG
CONFIG.SYS file	CONFIG.SIG
Information about the above files and their location on the hard disk	INFO.SIG

Examine your Critical Disk Area

Use *Examine* to check your local bootable drives for viruses. Examine compares your Critical Disk Area with an existing backup.

To examine your Critical Disk Area:

1. Select Protect Critical Disk Area from the Available Topics menu.

2. Select Examine from the Critical Area Options menu.

3. Select the drive to be examined.

4. Press ENTER.

   The Examine Activity screen will appear and the examination will begin.

If a virus or change is detected in the Critical Disk Area you can use a rescue diskette to restore the area. (First check to see if there is a reason for a change in the area, such as a new version of DOS.)

Restore your Critical Disk Area

Use *Restore* to recover from an infection or corruption of the Critical Disk Area.

NOTE:If you have a serious infection that will not allow you to boot your machine from the hard drive, see ‘Critical Disk Area Lost’ for instructions.

To use the Restore function:

1. Select Protect Critical Disk Area from the Available Topics menu.

2. Select Restore from the Critical Area Options menu.

3. Select the drive from which you want to restore.

   The best place to restore from is a rescue diskette. If you do not have one, your last choice should be from your local hard drive.

4. Press ENTER.

   The Restore Activity screen appears and the restoration begins.

Command line installation

The command line installation feature allows you to write a script program that will install Cheyenne AntiVirus for DOS to any DOS workstation in your network.

The DOS command line installation has the following syntax:

INSTALL *DESTINATION /OPTIONS*

Where *DESTINATION* is the workstation drive and path where the Cheyenne AntiVirus for DOS Manager will be installed.

You can specify one or more options. Options can be entered using a leading slash (/), dash (-) or space. For example, both of the following would produce the same results:

```
INSTALL C:\ANTIVIRUS /EXA /IMM /Q
```

```
INSTALL C:\ANTIVIRUS EXA IMM Q
```

The available are described below:

Option	Description
/EXA	Adds EXAMINE to your AUTOEXEC.BAT.
/Q	Installs Cheyenne AntiVirus in the Quiet Mode. Used in the system login script, this option automatically installs Cheyenne AntiVirus. It does not ask the user whether he or she would like to install.
/H	Displays help for the command line installation.

Option	Description
/IMM	Adds the IMMUNE TSR to your AUTOEXEC.BAT.

The /IMM option adds the IMMUNE TSR to your AUTOEXEC.BAT. You can include one or more of IMMUNE's options to the INSTALL command. The IMMUNE options are listed below:

IMMUNE (/IMM) Options	Description
/IMM options	
/ALL	Scans all files (not just executable files). This option requires a large amount of CPU resources.
/LC	Installs large IMMUNE in conventional memory.
/LE	Installs large IMMUNE in expanded memory. About 7K of conventional memory will also be used.
/LX	Installs large IMMUNE in extended memory. About 7K of conventional memory will also be used.
/M	Installs medium IMMUNE.
/N	Does not scan memory.
/HNG	Locks the workstation if a virus is found. This will prevent users from ignoring a virus message. If a virus is found, the workstation will have to be rebooted before proceeding. *Be aware that any unsaved information in open files will be lost!*
/NFS	Completely scans files. Without this option, IMMUNE only checks the beginning and end of files. Executable files (*.EXE, *.COM, etc.) are always fully scanned. This option requires a large amount of CPU resources.

IMMUNE (/IMM) Options	Description
/NOP	Does not scan files that are open.
/PR	Monitors your workstation for virus-like behavior, such as unauthorized formatting of your hard disk.
/XEN	Removes Enforcement for a workstation. Use if the workstation does not log in to an Cheyenne AntiVirus domain server. For memory management purposes, this option removes the Enforcement capability from IMMUNE. This option is solely for stand-alone environments.
/XHK	Does not rehook interrupt 21 for DOS. Use if you have other TSRs that consistently rehook to this interrupt.
/XLN	Disables all network communication features. Use for stand-alone workstations. This option reduces the size of IMMUNE.
/Q	Does not display messages while IMMUNE is loading.
/S	Loads the small version of IMMUNE.
/1	Scans 1 Meg of memory.

Following is an example of how you can use INSTALL:

```
A: INSTALL C:\ANTIVIRUS /EXA /IMM /M
```

This command runs Cheyenne AntiVirus's INSTALL program from a floppy A drive and installs the Cheyenne AntiVirus for DOS Manager to the Cheyenne AntiVirus directory on your local C drive. It also adds statements to the AUTOEXEC.BAT to execute EXAMINE and load the medium version of IMMUNE into memory when the workstation is booted.

10

Chapter

VIRUS RECOVERY PROCEDURES

When a virus strikes, it is vital that you follow proper recovery procedures. This chapter explains how to recover from various types of virus infections.

In this chapter, you will learn:

Page	
10-2 ➢	What to do if Cheyenne AntiVirus discovers a virus
10-3 ➢	What to do for an infected file or a virus in memory
10-4 ➢	What to do for a boot-sector virus
10-5 ➢	How to restore your Critical Disk Area

What to do if Cheyenne AntiVirus discovers a virus

Required items

You need the following in order to recover from a virus:

- Cheyenne AntiVirus for Windows Manager diskettes (and possibly the Cheyenne AntiVirus for DOS Manager diskette).
- A backup of the Critical Disk Area for the infected computer.
- A clean, write-protected, bootable floppy disk containing the operating system files that match the version of the operating system used when the Critical Disk Area was backed up.

It is very important to maintain a current set of Critical Disk Area files for all workstations. This backup may have been created in the following ways:

- A rescue diskette was created when Cheyenne AntiVirus was installed. The files reside on the rescue disk.
- The backup files were created automatically when an Cheyenne AntiVirus manager was installed and they reside in the Cheyenne AntiVirus home directory.
- EXAMINE /C was run. The files will reside wherever the Cheyenne AntiVirus environment is set.
- The Backup Critical Disk Area option was used. The location of the files is determined by the destination chosen when the backup is made, and can be either a floppy, master server in a domain, stand-alone server, or local hard disk. Files backed up to servers are stored in subdirectories of the Cheyenne AntiVirus home

directory. The subdirectory path is the network segment followed by the network interface card (NIC) address.

Infected file detected or an infection found in memory

If an infected file is detected or an infection is found in memory:

1. Exit the program you are in (be sure to save your work, if necessary).

2. Shut off the computer.

3. Boot your workstation with a write-protected, virus-free boot diskette (such as the original operating system diskette).

   The CONFIG.SYS on this diskette must have FILES=40 or a higher number. It is recommended that you also add the statement DEVICE=HIMEM.SYS. For this statement to work, you must copy the HIMEM.SYS file, located in the DOS directory, on to the diskette.

   If you do not have a CONFIG.SYS on your diskette, you can add the necessary information using the following procedure. *Since your own workstation may have already been infected, it is highly recommended that you do the following at another workstation which is infection free.* If no other workstation is available, perform the following AFTER booting your workstation with the boot diskette:

   - At the A prompt, type:

     ```
     COPY CON CONFIG.SYS   <ENTER>
     ```

   - With the cursor flashing, type:

     ```
     FILES=40
     DEVICE=HIMEM.SYS <F6>  <ENTER>
     ```

Note that you must disable write-protection to create the CONFIG.SYS file. After creating it, re-enable write-protection on the diskette.

- Re-boot your workstation.

4. Run the Cheyenne AntiVirus for Windows Manager or Cheyenne AntiVirus for DOS Manager.

5. Use the Local Scanner (in Windows) or Run Scanner (in DOS) to scan your hard drive.

6. Use the scanning report to delete any infected files identified (or scan again with the ‘Delete File’ option) and replace the files from a reliable source.

   The last resort should be to scan with the ‘Cure File’ option selected.

7. Re-scan the hard disk after replacing infected files to ensure the virus has been removed from the system.

Boot sector virus detected or suspected (EXAMINE fails)

If a boot sector virus is detected or suspected:

1. Cold-boot your workstation with a write-protected, virus-free boot diskette (such as the original operating system diskette).

   The CONFIG.SYS on this diskette must have FILES=40 or a higher number. It is recommended that you also add the statement DEVICE=HIMEM.SYS. For this statement to work, you must copy the HIMEM.SYS file, located in the DOS directory, on to the diskette.

   If you do not have a CONFIG.SYS on your diskette, you can add the necessary information using the following procedure. *Since your own workstation may have already been infected, it is highly recommended that you do the following at another workstation which is infection free.* If no other workstation is available, perform the following AFTER booting your workstation with the boot diskette:

- At the A prompt, type:

```
COPY CON CONFIG.SYS   <ENTER>
```

- With the cursor flashing, type:

```
FILES=40
DEVICE=HIMEM.SYS <F6>  <ENTER>
```

  Note that you must disable write-protection to create the CONFIG.SYS file. After creating it, re-enable write-protection on the diskette.

- Re-boot your workstation.

2. Run the Cheyenne AntiVirus for DOS Manager and restore the Critical Disk Area from any of the sources identified in the ‘Required items’ section.

3. Run EXAMINE to verify that no viruses are found in memory and that the Critical Disk Area has been properly restored.

Critical Disk Area lost

Depending on the degree of damage, a virus can alter all or part of the critical disk area. If all of the critical disk area is lost, the procedure to recover is as follows:

Restoring from a floppy disk

Be aware that the procedure below asks you to perform the same actions several times. It is important that all these steps are followed as outlined.

To restore from a floppy disk:

1. Cold boot from a clean, write-protected system floppy.

   The CONFIG.SYS on this diskette must have FILES=40 or a higher number. It is recommended that you also add the statement DEVICE=HIMEM.SYS. For this statement to work, you must copy the HIMEM.SYS file, located in the DOS directory, on to the diskette.

If you do not have a CONFIG.SYS on your diskette, you can add the necessary information using the following procedure. *Since your own workstation may have already been infected, it is highly recommended that you do the following at another workstation which is infection free.* If no other workstation is available, perform the following AFTER booting your workstation with the boot diskette:

- At the A prompt, type:

  ```
  COPY CON CONFIG.SYS   <ENTER>
  ```

- With the cursor flashing, type:

  ```
  FILES=40
  DEVICE=HIMEM.SYS <F6>  <ENTER>
  ```

  Note that you must disable write-protection to create the CONFIG.SYS file. After creating it, re-enable write-protection on the diskette.

- Re-boot your workstation.

2. Using the Cheyenne AntiVirus for DOS Manager, restore the Critical Disk Area.

   It will report as failed, but CMOS should be restored. Boot again from a floppy disk. The system should now recognize the existing hard drive.

3. Using the Cheyenne AntiVirus for DOS Manager, restore the Critical Disk Area.

   It will report as failed, but Partition information should now be restored. Boot again from a floppy disk.

4. Using the Cheyenne AntiVirus for DOS Manager, restore the Critical Disk Area.

   It will report as failed, but the Master boot sector should now be restored. Boot again from a floppy disk.

5. Using the Cheyenne AntiVirus for DOS Manager, restore the Critical Disk Area.

   System files should now be restored. You can now boot from your hard drive. All the hard drive information should be available. Run CHKDSK to verify this. There is a possibility that the virus also corrupted part or all of the information on the hard drive.

Restoring from a network

To restore from network:

1. If you haven't already, install the Cheyenne AntiVirus for DOS Manager to a directory on a server.

2. Boot the workstation from a clean, write-protected floppy disk. Include the network drivers (IPX, NETX or equivalent ODI/VLM drivers) on the floppy.

   The CONFIG.SYS on this diskette must have FILES=40 or a higher number. It is recommended that you also add the statement DEVICE=HIMEM.SYS. For this statement to work, you must copy the HIMEM.SYS file, located in the DOS directory, on to the diskette.

   If you do not have a CONFIG.SYS on your diskette, you can add the necessary information using the following procedure. *Since your own workstation may have already been infected, it is highly recommended that you do the following at another* *workstation which is infection free.* If no other workstation is available, perform the following AFTER booting your workstation with the boot diskette:

- At the A prompt, type:

```
COPY CON CONFIG.SYS   <ENTER>
```

- With the cursor flashing, type:

```
FILES=40
DEVICE=HIMEM.SYS <F6>  <ENTER>
```

  Note that you must disable write-protection to create the CONFIG.SYS file. After creating it, re-enable write-protection on the diskette.

- Re-boot your workstation.

3. Log in to the server where the Critical Disk Area backup files were made.

4. Change to the directory containing the Cheyenne AntiVirus for DOS Manager files.

5. Run the DOS Manager and restore as per the procedure detailed on the previous page in the ‘Restoring from a floppy disk’ section.

   Select the name of the server containing the backup files as your source.

11

Chapter

USING CHEYENNE ANTIVIRUS FOR MACINTOSH

This chapter explains how to install and use Cheyenne AntiVirus for MacIntosh.

In this chapter, you will learn:

Page

11-3 ➢ What Cheyenne AntiVirus for Macintosh is

11-4 ➢ How to install Cheyenne AntiVirus for Macintosh

11-7 ➢ How to use the Quick Start feature to quickly scan your Macintosh after Cheyenne AntiVirus is installed

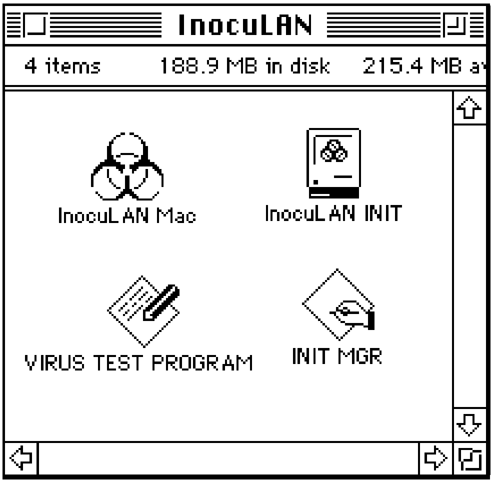
11-7 ➢ How to use Cheyenne AntiVirus for Macintosh

About Cheyenne AntiVirus for Macintosh

What is Cheyenne AntiVirus for Macintosh?

Cheyenne AntiVirus for Macintosh is a virus protection program that decontaminates and protects your Macintosh against known computer viruses. The Cheyenne AntiVirus for Macintosh application detects contaminated files, removes the virus and reverses any side effects, repairing the file.

Cheyenne AntiVirus for Macintosh consists of two primary pieces, the application program and the Cheyenne AntiVirus INIT. The application is what you run first, before doing anything else, to check for and remove viruses from your hard disk.



After you've “cleaned” your disk, you can place the INIT in your system extension folder. Once the Cheyenne InocuLAN INIT is active, any attempt to run a program contaminated with a known virus will result in a system error indicating that the file is already open. This will prevent the contaminated application from opening and spreading the virus.

Installing Cheyenne AntiVirus for Macintosh

This section provides you with the basic instructions for installing Cheyenne AntiVirus.

System Requirements

The Cheyenne AntiVirus for Macintosh application requires System software 6.0 or higher and 128K or 256K ROMs (these are the ROMs used in the Mac Plus, SE, II and above).

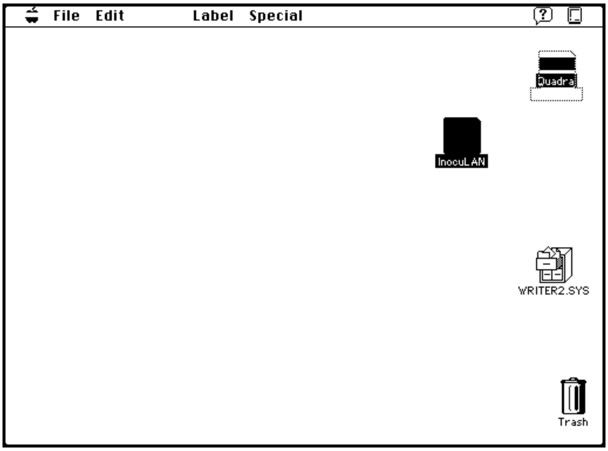
NOTE:Do not attempt to run this software with earlier System versions or on machines with 64K ROMs.

The Cheyenne AntiVirus for Macintosh application is fully MultiFinder compatible and will run in the background under MultiFinder.

To install the Cheyenne AntiVirus for Macintosh application:

1. Insert the Cheyenne AntiVirus CD-ROM into the drive.

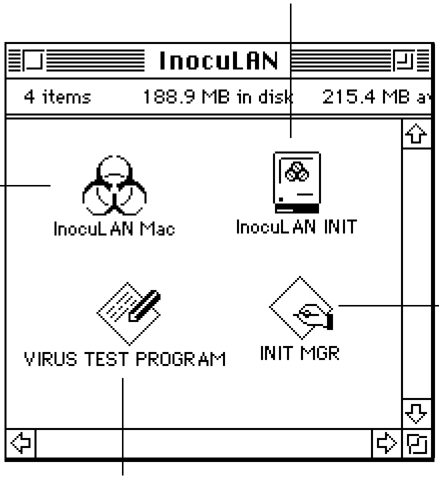
2. Copy the Cheyenne AntiVirus files to the hard disk by dragging the Cheyenne AntiVirus CD-ROM to your hard disk.



NOTE: You must keep the Cheyenne AntiVirus program and associated files in the Cheyenne folder for the INIT to work properly.

3. Open the Cheyenne AntiVirus folder (on your hard disk) by double clicking on it.

You see the following files:



This is the InocuLAN INIT. Put this in your System folder after you have checked for and removed viruses from your hard disk using the Cheyenne AntiVirus application.

This is the Cheyenne AntiVirus application. Run this to check and repair infected volumes, folders, files, and diskettes.

This is the INIT manager. Use this application to enable and disable the INIT after you've placed it in your system folder.

This is a test file that has all the characteristics of an infected file (don't worry, it doesn't actually contain a virus). Use it to test that the Cheyenne AntiVirus program and the INIT are working properly.

4. Scan your hard disk for viruses.

   See the following section 'Quick Start: Scanning your hard disk for viruses' for information about checking your hard disk.

5. Drag the INIT to your system folder.

   For more information about the INIT file, see 'About the Cheyenne AntiVirus for Macintosh INIT' later in this chapter.

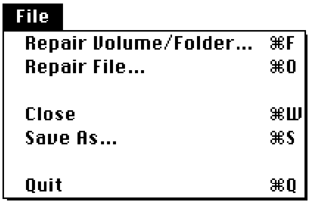
Quick Start: Scanning your hard disk for viruses

To quickly get started protecting your Macintosh, here is the minimum information necessary to use Cheyenne AntiVirus for Macintosh.

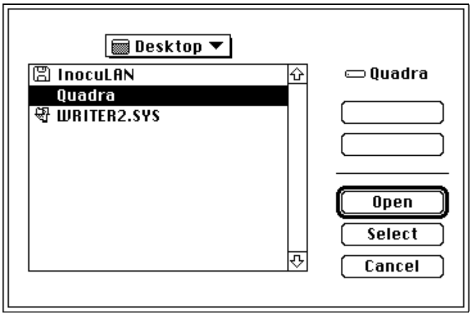
1. Start the Cheyenne AntiVirus for Macintosh application.

   Open the folder you installed on your hard disk and double-click the Cheyenne AntiVirus icon.

2. Select Repair Volume/Folder… from the File menu.

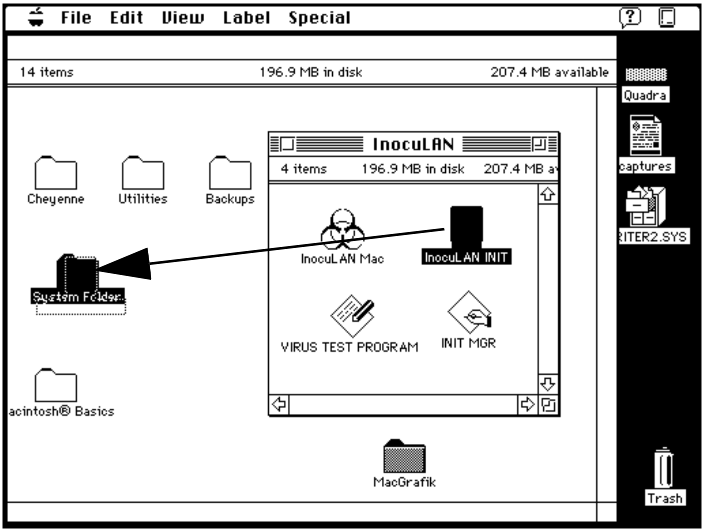


3. Select your normal startup volume (your hard disk) and click the Select button to check/repair it.



If you get an error from Cheyenne AntiVirus, such as “The file ‘Word’ is busy and could not be examined”, try closing the file (or application) that was busy and checking it again.

4. Drag the Cheyenne AntiVirus INIT into your System Folder.



You'll get a message telling you that this file must be placed in the Extensions folder. Click OK to put the INIT in the Extensions folder.

5. Restart your computer.

   Your disk is now free of all known viruses and the Cheyenne AntiVirus for Macintosh INIT prevents infection or re-infection by those viruses.

About the Cheyenne AntiVirus for Macintosh INIT

As mentioned before, Cheyenne AntiVirus for Macintosh consists of two primary pieces, the application program and the INIT.

The application is what you run first, before doing anything else, to check for and remove viruses from your hard disk. You should also use Cheyenne AntiVirus to scan diskettes, the first time you use them.

The INIT is what you copy into your system extensions folder after you've checked and repaired your disk with the Cheyenne AntiVirus for Macintosh program.

The INIT serves three primary purposes:

- ➢ To work in the background scanning files (as you try to execute them) for viruses.
- ➢ To prevent you from opening a file that is infected with a virus.
- ➢ To notify you through Alert.NLM when a virus is detected (if you have mounted a NetWare volume that is running the DOS/NetWare version of Cheyenne AntiVirus).

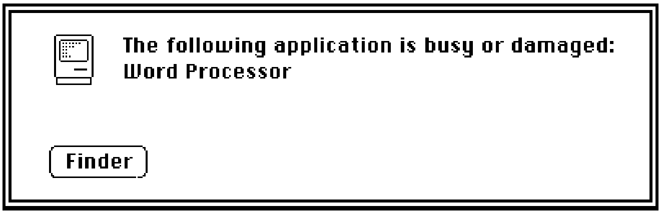
Receiving alert messages through a NetWare server

Alert is a Cheyenne program that runs on a NetWare server. It works with the InocuLAN.NLM to alert you of virus infections. Alert can inform you of virus infections using a number of methods including sending you a FAX, paging you, and sending you E-mail.

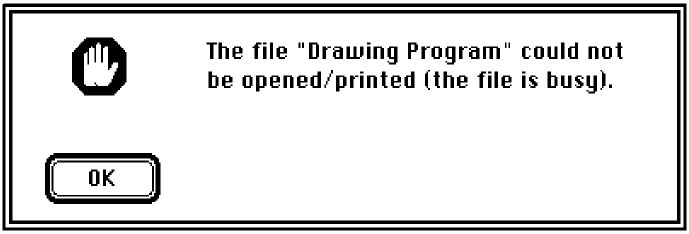
Again, you must have mounted a NetWare volume on your Macintosh that is running Cheyenne AntiVirus for DOS and Alert in order for INIT to notify you of viruses through the NetWare server.

If you try to run or open an infected file after you've installed the INIT in your system folder, a message similar to one of the following will appear:

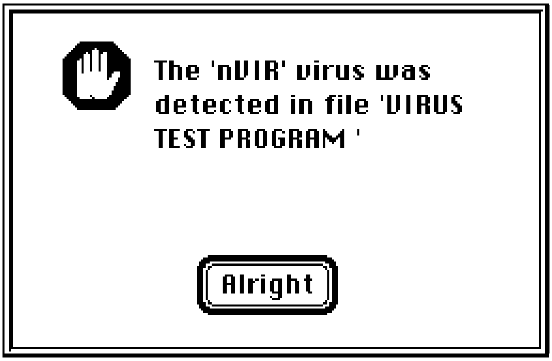
Typical message displayed by the finder when you try to use an infected file


The following application is busy or damaged:
Word Processor

Typical message displayed by MultiFinder when you try to use an infected


The file "Drawing Program" could not be opened/printed (the file is busy).

After you close the above dialog boxes, you should get another dialog box that gives you more details about the virus that has infected the file:



The 'nVIR' virus was detected in file 'VIRUS TEST PROGRAM '

Again, the Cheyenne AntiVirus for Macintosh INIT acts to prevent contamination by known viruses by generating a system error, indicating that a contaminated application is already open. This prevents the infected file from opening and the contamination from spreading, defeating the virus.

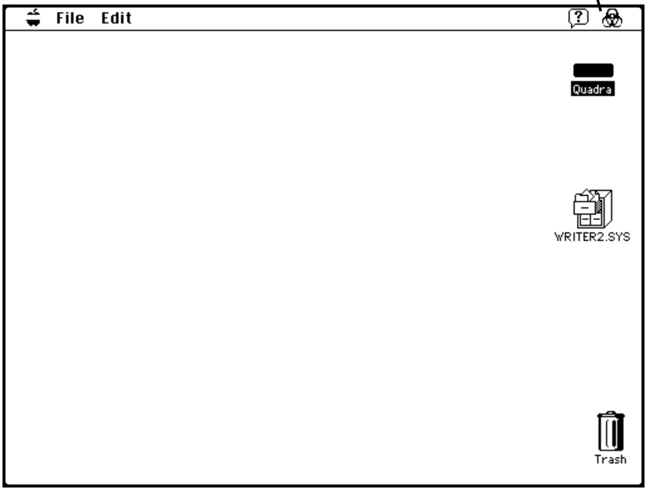
Immediately check any program that causes an “already open” error alert with the Cheyenne AntiVirus for Macintosh application.

Repairing volumes and folders

Follow these directions to check and repair an entire hard disk or folder:

1. Start Cheyenne AntiVirus for Macintosh by double clicking on the Cheyenne AntiVirus application icon.

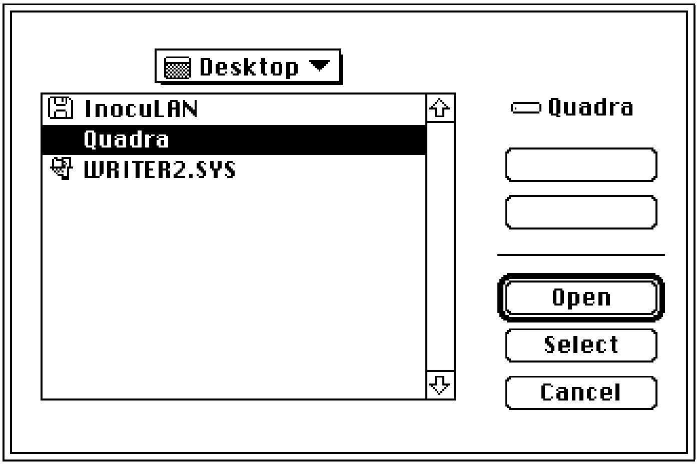
   The Cheyenne AntiVirus splash screen appears. Click anywhere on the splash screen to continue. Your desktop should look similar to the following:

   This icon indicates that Cheyenne AntiVirus is running.

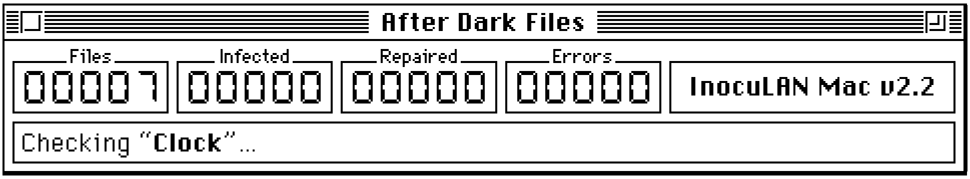
2. Select Repair Volume/Folder… from the File menu.

A dialog box similar to the following appears:



3. Select the volume (disk) or folder that you want to process and click “Select”.

   The Cheyenne AntiVirus for Macintosh application window shown below opens:



Files 00007 Infected 00000 Repaired 00000 Errors 00000

Checking “**Clock**”...

There are four counter fields:

- Files
- Infected
- Repaired
- Errors

To the right of the counter fields, a field displays the version number of Cheyenne AntiVirus for Macintosh. Always refer to this version number when contacting Cheyenne. Just below the counter fields, there is a field that displays the names of files as they are checked.

NOTE:You can stop Cheyenne AntiVirus for Macintosh at any time, in both check and repair modes, by pressing the command and period keys together.

The “Files” counter shows the number of files checked by Cheyenne AntiVirus for Macintosh. The “Infected” counter shows the number of infected files found and the “Repaired” counter shows the number of files that have been repaired by removing the viruses that had infected them. At the end of a successful Cheyenne AntiVirus for Macintosh run, the “Infected” and “Repaired” counters will always be equal.

The “Errors” counter shows the number of files that could not be checked or repaired because of an operating system condition such as “File Open”. If you get a “File Open” error, close the file and check it again.

NOTE:Note that all the counters show the number of files infected, repaired, or having an error reported. Therefore, a file that was infected with more than one virus would be counted only once in “Files”, “Infected” and “Repaired”. Simultaneous infection of an application by more that one virus is an increasingly common situation. Cheyenne AntiVirus for Macintosh has been designed to handle these cases.

After Cheyenne AntiVirus for Macintosh finishes checking the volume or folder, you can save the status screen (shown on the previous page) as a report. See the section, ‘Saving an Cheyenne AntiVirus for Macintosh log as a text file’ later in this chapter for more information.

Repairing Individual files

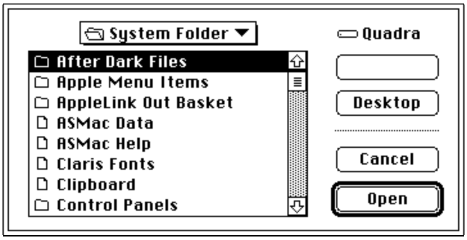
The Repair File command is used to process a single file. This is useful for verifying the safety of a new program added after an entire disk has been processed with Cheyenne AntiVirus for Macintosh.

Follow these directions to check an individual file:

1. Start Cheyenne AntiVirus for Macintosh.

2. Select Repair File... from the File menu.

   A dialog box similar to the following appears:



3. Select the file you want to check and click Open.

   Cheyenne AntiVirus for Macintosh scans the file. If the file is infected, it will remove the virus and repair the file. If the file is not infected, a message will appearing telling you this.

Repairing floppy disks

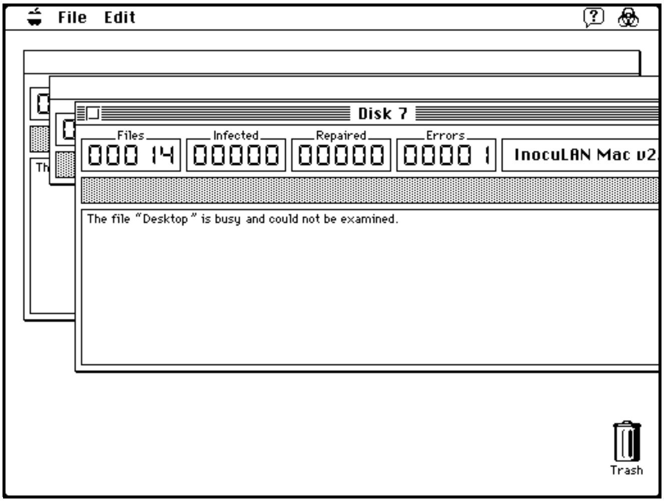
Follow these directions to check and repair floppy disks using Cheyenne AntiVirus for Macintosh.

1. Start Cheyenne AntiVirus for Macintosh.

2. Insert a disk in the disk drive.

   Whenever the Cheyenne AntiVirus for Macintosh application is running and active, a floppy disk is automatically processed as soon as you insert it in the disk drive. This has the same effect as selecting the Check Volume/Disk… command.

   As soon as the operation is completed, the disk is ejected. Inserting another disk will start another automatic repair, with a new report window "tiled" over that of the preceding disk. See below:

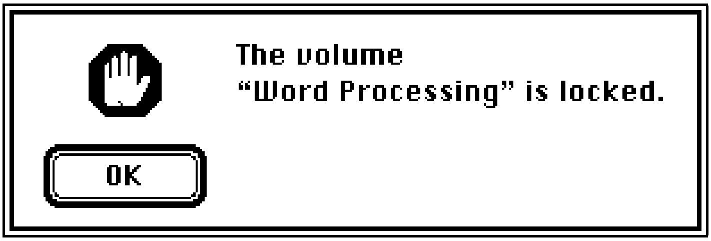


The file "Desktop" is busy and could not be examined.

Locked disks

Cheyenne AntiVirus for Macintosh cannot repair locked disks. When a locked floppy disk is inserted the

Cheyenne AntiVirus for Macintosh application is running, a message similar to the following will appear:



The volume
"Word Processing" is locked.

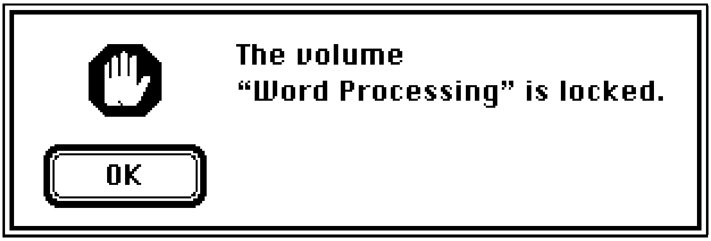
A floppy disk can be unlocked for processing by sliding the write protect tab to the write enable position. A CD-ROM disk, of course, is always locked. See the section, 'Checking Volumes and Files' for information on checking a CD-ROM disk.

Checking volumes and files

In normal operation, Cheyenne AntiVirus for Macintosh automatically repairs any contaminated files that it encounters by removing the virus and actively reconstructing damaged parts of the application.

NOTE:Under some special circumstances, it may be desirable to check a file or volume without automatically repairing (removing) viral infections. For example, checking without repairing may be a first step prior to obtaining permission to repair files.

Another case for simply checking files is checking a CD-ROM disk. CD-ROM disks are always “read only”. In the regular Cheyenne AntiVirus for Macintosh repair mode, a CD-ROM will always be a locked disk and Cheyenne AntiVirus for Macintosh will reject it, displaying the following dialog box:



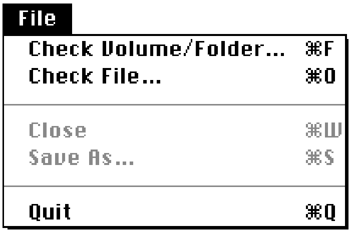
The volume
“Word Processing” is locked.

Using the Check Only option of Cheyenne AntiVirus for Macintosh will scan a CD-ROM for viruses, even though a disk of this type can never be repaired.

To use the Check option, follow these directions:

1. Hold down the Option key when pulling down the File menu.

The Repair Volume/Folder… and Repair File… commands will be replaced by Check Volume/ Folder… and Check File…, as shown below:



After this, Checking works exactly the same as repairing, that is you select what you want to check and Cheyenne AntiVirus does the rest. See ‘Repairing Volumes and folders’ and ‘Repairing individual files’ previously in this chapter for more information about using these options.

Checking diskettes

Diskettes can be automatically checked upon insertion.

To automatically check a diskette on insertion:

1. Hold down the option key when the disk is inserted.

   The option key does not have to be held down during the entire check. However, it must be held down whenever a disk is inserted, or that disk will be repaired, rather than checked.

Repairing or checking AppleShare servers

You can use Cheyenne AntiVirus for Macintosh to repair or check an AppleShare server. To check an AppleShare server, mount the server volume that you want to repair/check on your Macintosh then select the volume using Cheyenne AntiVirus’s Repair Volume/ Folder Option.

NOTE:The Cheyenne AntiVirus for Macintosh application can only check those files to which it has access. Therefore, to perform a complete check of a server volume, you must have supervisor or equivalent privileges on the AppleShare server.

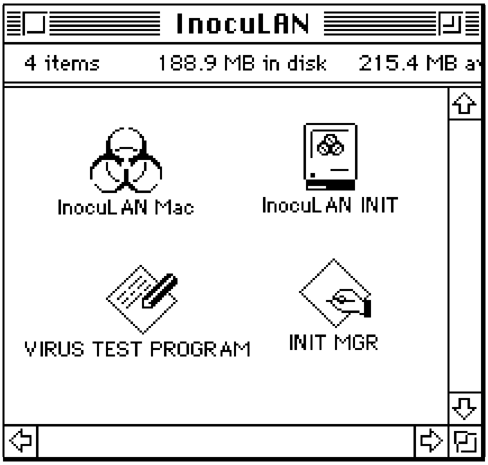
You can stop Cheyenne AntiVirus for Macintosh at any time, in both check and repair modes, by pressing the Command and Period keys together.

Using the INIT manager

The INIT manager (INIT MGR) allows you to enable and disable the Cheyenne AntiVirus for Macintosh INIT. The purpose of the INIT, once it is copied into your System folder, is to prevent you from opening an infected file. There may be times, however, when you absolutely must open an infected file. To do this, you will need to first disable the Cheyenne AntiVirus INIT.

To disable the Cheyenne AntiVirus INIT:

1. Start the INIT MGR.



2. Select Disable INIT from the File menu.

   You will now be able to open the infected file.

   The INIT will be disabled for one minute. After one minute, you will hear three beeps which mean the INIT is enabled again.

To enable the INIT:

Select Enable INIT from the File menu.

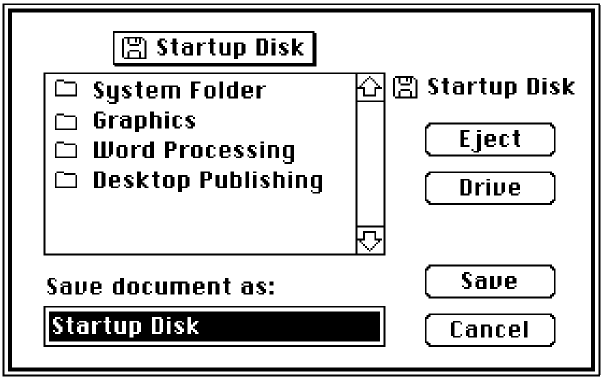
Saving a log as a text file

It is often desirable to keep a log of the files that were processed by Cheyenne AntiVirus for Macintosh. The log can be useful in tracing the source, history and consequences of viral infections.

Follow these directions to save a log to a text file:

1. Run repair or check on a volume, file or floppy disk.
2. After the job finishes, select Save As... from the File menu.

   A dialog box similar to the following will appear:



Save document as: Startup Disk

3. Enter a name for this log file and click Save.

   By default, Cheyenne AntiVirus uses the same name as the file/folder that you checked/repaired along with a.txt extension. It also places the file in the folder that you were just checking/repairing.

   You can open or print this text file with any word processor that accepts a text file.

A

Chapter

ABOUT COMPUTER VIRUSES

This appendix explains the basic concepts about computer virues.

In this chapter, you will learn:

Page	
A-3 ➢	What is a computer virus?
A-3 ➢	Where do viruses come from?
A-3 ➢	How to tell if your computer has a virus
A-5 ➢	What a virus can do to your computer
A-5 ➢	Type of viruses

A-7 ➢ Characteristics of viruses

What Is a Computer Virus?

A computer virus is a computer program that can destroy information on your workstation. Similar to a biological virus, a computer virus can reproduce itself by attaching to other files, usually executable programs. When isolated (unexecuted, such as in a compressed file), computer viruses are not dangerous, but when they are opened, they can create havoc.

In order to be classified as a virus, a suspicious file must have the following characteristics:s

- ➢ replicates itself
- ➢ attaches itself to other executables

How does your workstation get a virus?

Viruses are transmitted when an infected file is copied, downloaded, or used.

About 80% of viruses are transmitted by disk. Sometimes, off-the-shelf software contains viruses. If the virus is a “Boot Sector virus,” it is spread when a workstation is mistakenly booted up with the infected disk.

About 20% of viruses are transmitted by modem. Sometimes unsecured bulletin boards are the source of viruses and infected files are passed directly to a workstation.

How can you tell if your computer has a virus?

Symptoms of viral infection vary depending upon the particular virus infecting your system. The following list contains some of the more common symptoms you are likely to encounter:

- Your screen displays a message such as “Your PC is now Stoned!”
- Your screen displays strange graphic patterns, such as bouncing balls.
- Files increase in size. Sometimes this is dramatic, causing the files to become too big to be loaded in memory. Frequently the change in size is small.
- The time stamp on a file is changed. You may notice a .COM or .EXE file with a time stamp more recent than when you loaded it.
- You get an error message about writing to a write-protected disk, even though your application is not attempting a write operation.
- It takes longer to load programs and your computer’s configuration has not changed.
- Your computer seems to be running much slower than normal.
- Your computer has less memory available than normal.
- The same type of problems are occurring on several computers.
- You get a “Bad command or file name” error even when you know the file should be on the disk.
- You cannot access a drive that you know exists.
- CHKDSK suddenly discovers bad sectors on more than one computer.
- You are having persistent problems on your computer, such as difficulty in copying files.

- Your computer locks up frequently.

If your computer exhibits one or more of these symptoms, you may have a virus infection. Since it can be difficult to determine if these symptoms are virus-related, we suggest you use Cheyenne AntiVirus to confirm whether or not your workstation is infected.

What can a virus do to your computer?

Not all viruses damage your computer. Some viruses are just nuisances, continually reproducing themselves or displaying strange graphics or messages on your screen.

Most viruses are stealthy, remaining hidden until they start running.

If a virus does cause damage, the damage will vary depending upon the particular virus infecting your system. In general, viruses can do the following damage to your computer:

- Hang your computer.
- Erase your files.
- Scramble data on your hard disk.
- Attack the File Allocation Table (FAT).
- Attack the Partition Table
- Format your hard disk.

Types of viruses

Viruses are classified according to how the virus is transmitted and how it infects the computer.

- Boot Sector viruses - These viruses overwrite the disk’s original boot sector (which contains code that is executed when the system is booted) with its own code so that the virus is always loaded into memory before anything else. This means that every time you start your computer, the virus is run. Once in memory, the virus can make your startup disk unusable or can spread to other disks.

- Master Boot Sector viruses - These viruses overwrite the disk's master boot sector (partition table). These viruses are difficult to detect because many disk examination tools do not let you see the partition sector, which is the first sector on a hard disk.
- Macro viruses - These viruses are written in the macro language of specific computer programs, such as a word processor or spreadsheet. Macro viruses infect files (not the boot sector or partition table), and can become memory resident when executed. They can be run when a program document is accessed, or triggered by user actions, such as certain keystrokes or menu choices. Macro viruses can be stored in files with any extension and are spread via file transfers, even over e-Mail.
- File viruses -These viruses infect other programs when an infected program is run. They do not remain in memory, so they do not infect the system. Like Memory Resident viruses, Non-Resident viruses attach themselves to executable files. These viruses often change the file attribute information and the file size, time, and date information.

- Multipartite viruses - These viruses combine the characteristics of Memory Resident, File, and Boot Sector viruses.

Characteristics of viruses

The types of viruses listed above may exhibit different behavioral characteristics, based on how they function.

- Memory Resident viruses - These viruses load themselves in memory and take over control of the operating system. Memory Resident viruses attach themselves to executable files (such as .EXE, .COM, and .SYS files). These viruses often change the file attribute information and the file size, time, and date information.
- Stealth viruses - These viruses hide their presence. While all viruses try to conceal themselves in some way, Stealth viruses make a greater effort at concealment. For example, a stealth virus can infect a program, adding bytes to the infected file. It then subtracts the directory entry of the infected file by the same number of bytes, giving the impression that the file’s size has not changed.
- Polymorphic viruses - These viruses modify their appearance and change their signature (their identifiable code) periodically. For example, they may insert garbage code into the middle of a file execution, or change the order of execution. This allows the virus to escape signature scanning detection methods.

INDEX

A

- About Password Protection 6-8
- Account
  - Service connections 5-6
- Activity Log
  - Alert 5-32
- Alert 11-9
  - Basics 5-2
  - Broadcast options 5-11
  - Configuration 5-6
  - Configurations 5-6
  - E-mail 5-12, 5-19
  - Event logs 5-32
  - Events logs 5-33
  - Fax recipients 5-12
  - Features 5-2, 5-3
  - Log 5-32
  - Macintosh 11-9
  - Manager 5-4
  - Options
    - pager 5-12
  - Pager messages 5-14
  - Pager option 5-12
  - Pager recipients 5-12
  - Port configuration 5-14
  - Services 5-6
  - SNMP 5-16, 5-23, 5-26
  - Trouble Tickets 5-18
- Alert System 1-7
- AntiVirus
  - DOS 9-3, 9-10
  - How does AntiVirus work? 1-4
  - Macintosh 11-1, 11-3
    - INIT 11-3
    - Install 11-4
    - Logs 11-22
    - Quick start 11-7
    - Recovery 11-12, 11-16
    - System requirements 11-4
  - Prevention methods 1-4
  - Product Description 1-3
  - Product features 1-5
  - Recovery 10-2
  - Updating 7-23
  - Windows 31x 8-15
    - Installation 8-3, 8-4, 8-6
    - System requirements 8-3
  - Windows 95 6-2, 6-10, 6-11
    - Installation 6-3
    - Signature file 7-23
    - System requirements 6-3
    - Virus engine 7-23
- antivirus options 1-6
- ARJ
  - Incoming Files 1-7
- Auto Download Manager 4-5
- AutoDownload
  - Configuration 7-26
- AutoDownload Manager 7-24
- AUTOEXEC.BAT 9-4, 9-6
  - Backup 7-18
  - Windows 31x 8-8, 8-9, 8-13
- AVUPDATE.INI 4-23

B

- Backup
  - AUTOEXEC.BAT 7-18
  - Boot sector 7-18
  - CMOS 7-18
  - CONFIG.SYS 7-18
  - Critical Disk 7-15, 8-13
- Batch file 8-36
- Boot disk
  - Critical Disk 7-14
- Boot sector
  - Backup 7-18
  - Viruses 7-21
- Boot Sector virus A-5
- Broadcast
  - Alert 5-4
  - Options 5-11

  - Services configuration 3-11
- Broadcast recipients 5-11
- Broadcasting messages 3-12
- Browser
  - InocuLAN 1-7
  - Internet Download 2-50
  - Windows 95 6-11, 6-17
  - Windows NT
    - Shell extension 2-49

C

- CD-ROM protection 1-6
- Cheyenne BBS 7-23
- Client
  - Windows 95 6-4, 6-11
- CMOS
  - Backup 7-18
- Command line
  - EXAMINE 8-46
  - Windows 31x 8-30
  - Windows 95 6-19, 6-26
- Command line installation 9-46
- Compressed Files 1-7
- Compression
  - Windows NT 2-47
- Computer Viruses A-1
- Computer viruses
  - Viruses 1-2
- CONFIG.SYS
  - Backup 7-18
  - Windows 31x 8-4
- Configuration
  - Alert 5-6
  - AutoDownload 7-26
  - Broadcast services 3-11
  - Communication ports 5-14
  - InocuLAN
    - Service manager 3-4
  - Macintosh
    - Alert 11-9
  - Network broadcasts 3-12
  - Pager 5-12
    - ID 5-13
    - Number 5-13
    - Type 5-13
  - Service manager 3-4
    - Event logs 3-6
  - TCP/IP 3-11
  - Trouble Tickets 5-18
  - Windows 95 6-12
  - Windows NT
    - System requirements 2-3
- configuration 2-10
- Configuring Software Distribution 4-12
- Configuring the Virus Directory Purge 3-10
- Creating the domain 2-8
- Critical Disk 7-14
  - Backup 7-15
  - Damage 7-21
  - DOS 9-42
    - Restore 9-45
  - Examining 8-44
  - Protecting 7-14
  - Windows 31x 8-13, 8-41
    - Restore 8-45
- Custom Setup
  - Windows 31x 8-8

D

- Domain
  - Security 2-27
- Domain Manager 2-7
- Domain Support 1-7
- DOS 9-10
  - AUTOEXEC.BAT 9-3
  - Critical Disk 9-42
    - Backup 9-43
    - Examining 9-44
    - Restore 9-45
  - Entering information 9-14
  - Help menu 9-19

IMMUNE 9-32
Installation 9-3
Keys 9-16
Mouse 9-18
Options 9-24
Scanner 9-24
Results 9-29
Screen types 9-11
Switching tasks 9-21
Text entry fields 9-13
Version information 9-20
Virus list 9-22
DOS command line
Windows 95 6-26
Download
Signature file 7-30
Downloading files 7-23

E

E-mail 5-12, 5-19
Environment variable
Configuration 9-9
Event Logs 5-33
Event logs
Filter 3-6
purge 3-6
EXAMINE 8-46
Options 8-46, 9-38
Explorer
Shell extensions 6-17
Windows 95 scanner 6-11
Windows NT shell 2-49

F

Fax recipients 5-12
File viruses A-6
Files
Windows 95 scanner 6-11
Windows NT
Compression 2-47
Floppy disk
Restore 10-5
Floppy-drive protection 1-5
ftp
AutoDownload 7-26
FTP Setting 4-9

G

Groupware Messaging 1-6
Groupware Options 1-6

H

Hardware requirements 8-3
Heartbeat intervals 3-14

I

IMMUNE 9-33
Defaults 9-34
Memory requirements 9-32
Options 9-34
Overview 9-32
Unloading 9-36
Versions 9-32
INIT 11-3
INOCUCMD 8-30
InocuLAN
Alert 5-2
Automatic configuration 3-11
Client install 2-3
Heartbeat 3-14
Service manager 3-3
TCP/IP 3-11, 3-13
Time-out 3-13
Installation
AntiVirus
Macintosh 11-4
Windows 31x 8-3, 8-4, 8-6

    - Windows 95 6-3
  - Command line 9-46
  - DOS manager 9-3
  - InocuLAN
    - Windows NT Client 2-3
  - PATH configuration 9-9
  - Windows 31x
    - CONFIG.SYS 8-4
  - Windows 95 client 6-4
- Internet
  - Download protection 2-50
- Internet Scanning 1-6

L

- Local Scanner
  - Options 8-23
  - Results 8-28
- login script 4-23
- Logs
  - Alert 5-32
  - Alert events 5-32, 5-33
  - Event filters 3-6
  - Events
    - Purge 3-6
  - Macintosh 11-22
  - Scan
    - Filters 3-8
    - Purge 3-8
  - Service manager 3-8
  - Windows 95 6-16
  - Windows NT
    - Results 2-48
- Lotus Notes Recipients 5-25
- Lotus Notes Settings 5-24

M

- Macintosh 11-9
  - AntiVirus
    - INIT 11-3
    - Installing 11-4
    - Overview 11-3
    - Volumes and folders 11-12
  - AppleShare servers 11-20
  - Checking diskettes 11-19
  - Checking volumes and files 11-18
  - INIT 11-9
  - INIT manager 11-21
  - Locked disks 11-16
  - Logs 11-22
  - Quick start 11-7
  - Recovery
    - Floppy disks 11-16
  - Repairing individual files 11-15
  - Repairing volumes and folders 11-12
  - Scanning hard disk 11-7
  - System requirements 11-4
- Mailslots 3-11, 3-15
- Mapped Drives
  - Windows 95 6-18
- Master Boot Sector virus A-6
- Memory
  - virus 10-3
- Memory requirements 8-3
- Memory Resident virus A-7
- Message
  - Event logs
    - Filters 3-6
  - Scan log 3-8
- Microsoft BackOffice 1-6
- Modem 4-9
  - AutoDownload 7-26
  - Configuration 5-14
- Modify a scan job 2-24
- Mouse
  - DOS 9-18
- Multipartite viruses A-7
- Multi-platform support 1-6

N

Network
- Macintosh 11-9
- Restore from 10-7
- TCP/IP 3-13
- Time-out 3-13

Network broadcasts 3-12
Network drive protection 1-6

O

Online
- AutoDownload 7-26

Online help 9-19
Options
- InocuLAN 1-7

P

Pager 5-12
- ID 5-13
- Interpreting messages 5-14
- Number 5-13
- Option 5-12
- Type 5-13

Pager messages 5-14
Pager recipients 5-12
Point-To-Point management 2-25
Polymorphic virus A-7
Prevention
- Critical Disk 7-14

Purge
- Event logs 3-6
- Scan log 3-8

Q

Quick Access 8-17
Quick access
- Windows 95 6-10

Quick start 11-7

R

Real-time
- WIMMUNE 8-39

Real-Time Copy Cure 1-7
Real-time Monitor 2-10
Real-Time protection 2-10
Real-time virus protection, see WIMMUNE 7-5
Recovering from a virus 7-19
Recovery
- Critical Disk 7-21
- Network 10-7
- viruses 10-2

Requirements 8-3
Restore
- DOS 9-45
- Floppy disk 10-5

S

Scan
- Logs
  - Filters 3-8
  - Purge 3-8
- Windows 95
  - Mapped Drives 6-18
- Windows NT
  - Results 2-48

Scan action
- Windows 95 6-12
- Windows NT 2-45

Scan log
- Windows 95 6-16

Scan type
- Windows 95 6-13

Scanner
- DOS 9-10, 9-24
  - Keys 9-16

Dos
Options 9-24
Screens 9-11
Windows 31x 8-30
Windows 95 6-11
Command line 6-19
Options 6-12
Windows NT 2-44
Scan type 2-46
Scanning action 2-11
Scheduled Updates
Windows NT 7-30
Scheduling 6-22
Windows 95 6-22
Scheduling the domain scan 2-14, 2-19
Security for domains 2-27
Server
Automatic configuration 3-11
Heartbeat 3-14
InocuLAN
Service manager 3-3
Server virus wall 1-5, 2-13
Service manager 3-3
Configuring Inoculan 3-4
Configuring the Event Log 3-6
Scan Log 3-8
Shell extensions
Windows 95 6-17
Windows NT 2-49
Signature Download and Distribution 4-2
Signature file updating 7-23
SNMP 5-16, 5-23, 5-26
Managers 5-16, 5-23, 5-26
Software requirements 8-3
Software Update and Distribution 1-7
Stealth virus A-7
System requirements
Macintosh 11-4
Windows 31x 8-3
Windows 95 6-3
Windows NT client 2-3

T

TCP/IP 3-11, 3-13
Tips
Viruses 7-4
TNG Alert Scenarios 5-30
TNG Recipients 5-28
Trouble Tickets 5-18
Configuration 5-18

U

Uninstalling
Windows 95 6-9
Update the login script 4-26
Updating AntiVirus 7-23
Utility
EXAMINE 8-46

V

Virus
Windows 95 scanner 6-11
Virus description 7-23
Virus Detection Code 5-15
Virus engine 7-23
Virus list 7-23, 9-22
Virus Quarantine 1-5
Virus quarantine 2-13
Virus Recovery Procedures 10-1
Virus signature 7-23
Viruses
Boot sector 7-21, 10-4
Computer viruses 1-2
Damage caused A-5
Definition A-3
How does AntiVirus work? 1-4
Infection 7-19
Memory 10-3
Prevention methods 1-4
Recover 7-19

Recovering from infection 10-2
Source of infection A-3
Suggestions 7-4
Symptoms A-3
Updating signature files 7-23

W

WIMMUNE 8-39
Automatic loading 7-5
Overview 7-5
Windows 31x
AntiVirus 8-15
AUTOEXEC.BAT 8-8, 8-9, 8-13
Command line 8-30
Critical Disk
Backup 8-41
Examining 8-44
Custom setup 8-8
Installation 8-3, 8-4, 8-6
Quick Access 8-17
Restore
Critical Disk 8-45
Scanner 8-30
System requirements 8-3
WIMMUNE 8-39
Windows 95
AntiVirus 6-2, 6-10
AntiVirus installation 6-3
AutoDownload 7-24, 7-26
Client Install 6-4
Command line 6-19
DOS command line 6-26
Installation 6-4
Quick access 6-10
Scan action 6-12
Scan log 6-16
Scan type 6-13
Scanner 6-11
Options 6-12
Scanning mapped drives 6-18
Scheduling jobs 6-22
Shell extensions 6-17
System requirements 6-3
Uninstalling 6-9
Windows manager
Domains
Actions for scanning 2-33
Job Queue 2-41
Message filters 2-43
Modifying a scan job 2-39
Progress of scan 2-41
Results of scanning 2-42
Scanning procedure 2-29
Local Scanner
Options 8-23
Results 8-28
Scan procedure 8-20
Windows NT
4.0 Support 1-6
Alert 5-2
Alert configuration 5-6
Alert Features 5-2
Alert manager 5-4
Alert services 5-6
Compression 2-47
InocuLAN Client installation 2-3
Internet download 2-50
Scan action 2-45
Scan results 2-48
Scan type 2-46
Scanner 2-44
Service Account 5-6
Service manager 3-3
Shell extensions 2-49
System requirements 2-3

Z

ZIP
Compressed Files 1-7